

---

# **NETKROM AIR-BR500G/GH**



## **User's Manual**

---

## Technical Support Information

The warranty information and registration form are found in the Quick Install Guide.

For technical support, you may contact Netkrom Technologies Inc. For your convenience, you may also seek technical assistance from the local distributor, or from the authorized dealer/reseller that you have purchased this product from. For technical support by email, write [support@netkrom.com](mailto:support@netkrom.com).

### SALES

Address:

Netkrom Technologies Inc.  
3152 NW 72nd Ave Miami,  
FL 33122 U.S.A.

Phone: +1 305-4182232  
Fax: +1 305-4189266  
Email: [sales@netkrom.com](mailto:sales@netkrom.com)

### TECHNICAL SUPPORT

Address:

Netkrom Technologies Inc.  
3152 NW 72nd Ave Miami,  
FL 33122 U.S.A.

Phone: +1 305-4182232  
Fax: +1 305-4189266  
Email: [support@netkrom.com](mailto:support@netkrom.com)

### INTERNET

Web:

[www.netkrom.com](http://www.netkrom.com)

---

## About This Document

The product described in this document, Outdoor Access Point Bridge, Netkrom AIR-BR500G/GH is a licensed product of Netkrom Technologies. This document contains instructions for installing, configuring and using Netkrom AIR-BR500G/GH. It also gives an overview of the key applications and the networking concepts with respect to the product.

This documentation is for both Network Administrators and the end user who possesses some basic knowledge in the networking structure and protocols.

It makes a few assumptions that the host computer has already been installed with TCP/IP and already up & running and accessing the Internet. Procedures for Windows 98SE/ME/2000/XP operating systems are included in this document. However, for other operating system, you may need to refer to your operating system's documentation for networking.

## How to Use this Document

The document is written in such a way that you as a user will find it convenient to find specific information pertaining to the product. It comprises of chapters that explain in details on the installation and configuration.

## Conventions

In this document, special conventions are used to help and present the information clearly. Below is a list of conventions used throughout.



### NOTE

This section will consist of important features or instructions

---



### CAUTION

This section concerns risk of injury, system damage or loss of data

---



### WARNING

This section concerns risk of severe injury

---

References on Menu Command, Push Button, Radio Button, LED and Label appear in **Bold**. For example, "Click on **Ok**."

---

<b>Technical Support Information.....</b>	<b>II</b>
<b>About This Document .....</b>	<b>III</b>
<b>How to Use this Document .....</b>	<b>III</b>
<b>Conventions .....</b>	<b>III</b>

<b>Chapter 1    Product Overview.....</b>	<b>1</b>
---	----------

<b>1.1    Introduction .....</b>	<b>1</b>
<b>1.2    Features and Benefits.....</b>	<b>1</b>
<b>1.3    Netkrom AIR-BR500G/GH Package .....</b>	<b>3</b>
<b>1.4    When to use which mode .....</b>	<b>3</b>
1.4.1    The Access Point Mode .....	4
1.4.2    The Access Point Client Mode.....	4
1.4.3    The Gateway Mode.....	5
1.4.4    The Wireless Routing Client Mode .....	6
1.4.5    The Wireless Ethernet Adapter Mode.....	7
1.4.6    The Wireless Bridge Link Mode.....	7

<b>Chapter 2    Hardware Installation.....</b>	<b>8</b>
--	----------

<b>2.1    Setup Requirements .....</b>	<b>8</b>
<b>2.2    Netkrom AIR-BR500G/GH Hardware Installation .....</b>	<b>8</b>

<b>Chapter 3    Access to Web-based Interface.....</b>	<b>9</b>
--	----------

<b>3.1    Access to the Web interface with uConfig.....</b>	<b>9</b>
<b>3.2    Verify the IP address of Netkrom AIR-BR500G/GH - The NpFind Utility .....</b>	<b>11</b>
<b>3.3    Direct access to web-based interface via Internet Explorer.....</b>	<b>12</b>

<b>Chapter 4    Common Configuration.....</b>	<b>18</b>
---	-----------

<b>4.1    Management Port Setup .....</b>	<b>18</b>
4.1.1    To view the active DHCP leases.....	20
4.1.2    To reserve specific IP addresses for predetermined DHCP clients .....	21
<b>4.2    WLAN Setup .....</b>	<b>24</b>
4.2.1    To configure the Basic setup of the wireless mode.....	24
4.2.2    To configure the Advanced setup of the wireless mode.....	27
<b>4.3    Scan for Site Survey (For Wireless Client Mode Only).....</b>	<b>30</b>
4.3.1    Show Link Information (For Wireless Client Mode Only) .....	31
<b>4.4    Wireless Extended Features .....</b>	<b>32</b>
4.4.1    Access Control – The Wireless Pseudo VLAN.....	32
4.4.2    Wireless Setup - The Wireless Distributed System (WDS) .....	40
4.4.3    WMM Parameters (available in all modes except for Wireless Bridge Link).....	46
4.4.4    Long Distance Parameters (available in all modes) .....	48
<b>4.5    WLAN Security .....</b>	<b>50</b>

---

4.5.1	How to set up WEP [Available in ALL modes].....	51
4.5.2	How to set up WPA-PSK [Available in AP/Gateway mode ONLY].....	53
4.5.3	How to set up 802.1x/RADIUS [Available in Access Point mode ONLY].....	54
4.5.4	How to set up WPA EAP [Available in Access Point mode ONLY].....	55
<b>4.6</b>	<b>STP Setup ( available in AP/Gateway modes).....</b>	<b>57</b>
<b>4.7</b>	<b>SNMP Setup.....</b>	<b>63</b>
<b>4.8</b>	<b>MAC Filtering .....</b>	<b>63</b>
 <b>Chapter 5 Further Configuration .....</b>		<b>65</b>
<b>5.1</b>	<b>Setting up uConfig (only in Gateway mode) .....</b>	<b>65</b>
<b>5.2</b>	<b>Configuring WAN Setup (Available in Gateway and Wireless Routing Client mode).....</b>	<b>66</b>
5.2.1	Dynamic IP .....	67
5.2.2	Static IP .....	67
5.2.3	PPPoE.....	68
5.2.4	Singapore ADSL.....	70
5.2.5	Australia BPA Cable.....	71
5.2.6	PPTP .....	72
<b>5.3</b>	<b>Using NAT (Only available in Gateway and Wireless Routing Client mode) .....</b>	<b>73</b>
5.3.1	To set up a De-Militarised Zone host.....	74
5.3.2	To set up port forwarding .....	75
<b>5.4</b>	<b>Routing (Only available in Gateway and Wireless Routing Client mode).....</b>	<b>78</b>
5.4.1	Static Routing .....	80
5.4.2	Dynamic Routing.....	81
<b>5.5</b>	<b>Implementing IP Filtering (Only available in Gateway and Wireless Routing Client mode) 82</b>	
<b>5.6</b>	<b>Applying Remote Management (Only available in Gateway and Wireless Routing Client mode).....</b>	<b>87</b>
<b>5.7</b>	<b>Enabling Parallel Broadband (Only available in Gateway mode) .....</b>	<b>88</b>
5.7.1	Load balancing.....	88
5.7.2	Fail-Over Redundancy .....	88
5.7.3	To enable Parallel Broadband .....	89
 <b>Chapter 6 System Utilities .....</b>		<b>91</b>
<b>6.1</b>	<b>Using the SYSTEM TOOLS Menu.....</b>	<b>91</b>
6.1.1	System Identity .....	91
6.1.2	WLAN Station List (Only available in AP and Gateway mode).....	92
6.1.3	Set System's Clock .....	92
6.1.4	Firmware Upgrade .....	93
6.1.5	Save or Reset Settings.....	94
6.1.6	Reboot System.....	95
6.1.7	Change Password.....	96
6.1.8	Logout.....	96
<b>6.2</b>	<b>Using the HELP menu .....</b>	<b>97</b>
6.2.1	Get Technical Support .....	97

---

6.2.2 About System .....	97
--------------------------	----

<b>Appendix I Troubleshooting.....</b>	<b>98</b>
--	-----------

<b>AI Solutions to Common Problems .....</b>	<b>98</b>
--	-----------

<b>Appendix II Firmware Recovery .....</b>	<b>102</b>
--	------------

<b>AII How to recover Netkrom AIR-BR500G/GH from failed firmware.....</b>	<b>102</b>
---	------------

## **1.1      Introduction**

The Netkrom AIR-BR500G/GH is a wireless outdoor access point that is interoperable with all standard based 802.11a, 11g and 802.11b wireless devices. The Netkrom AIR-BR500G/GH is a compact and high performance outdoor access point that is designed with support for high security features like Wi-Fi Protected Access (WPA), IEEE 802.1x Authentication and 64-bit or 128-bit Wired Equivalent Privacy. Netkrom exclusive wireless LAN technology Wireless Pseudo VLAN further enhances security in wireless hotspot networks in isolating different users into their own VLANs. The Netkrom AIR-BR500G/GH is capable of operating in 6 different modes: Access Point Bridging, Access Point Client, Gateway, Wireless Routing Client, Wireless Ethernet Adapter and Wireless Bridge Link; making it suitable for all kinds of wireless applications.

## **1.2      Features and Benefits**

Netkrom AIR-BR500G/GH has been designed for high performance and offers a rich suite of features, with which you should acquaint yourself to be able to exploit your Netkrom AIR-BR500G/GH's full potential

- **Wireless Distribution System**

This unique feature allows linking of several access points, virtually creating a larger wireless network infrastructure that allows desktops or laptops that are connected to Netkrom AIR-BR500G/GH to share their network resources wirelessly.

- **Pseudo Virtual LAN**

Netkrom AIR-BR500G/GH unique Wireless Pseudo Virtual LAN technology is a feature that allows a wireless client or groups of wireless client to be segmented wirelessly into its individual workgroup or individual node thus enhancing the privacy of the wireless clients. This is especially useful in public hotspot deployment.

- **Secured Wireless Authentication**

The Netkrom AIR-BR500G/GH supports the latest wireless security standard—Wi-Fi Protected Access. The wireless users now enjoy the freedom of wireless roaming without worrying important data being exposed to outsiders. WPA has two different modes: WPA-PSK for SOHO users and WPA-EAP for Enterprise users. NETKROM AIR-BR500G/GH supports WPA-PSK and WPA-EAP that using IEEE 802.1x-based Extensible Authentication Protocol (EAP) for secure and centralized user-based authentication. The wireless clients are now able to authentication through a RADIUS server to the authorized network through highly secured authentication methods like EAP-TLS, EAP-TTLS, and EAP-PEAP.

- **Smart Select**  
This feature will automatically scan and recommend the best channel that the access point can utilize.
- **Wireless Routing Client Capability**  
The Wireless Routing Client mode enables Internet Service Provider (ISP) or offices to send their data packet wirelessly and these network packets will be routed to a wired Local Area Network via the NETKROM AIR-BR500G/GH.
- **Wireless Ethernet Adapter**  
The Wireless Ethernet Adapter mode enables any computers with an Ethernet interface to be connected to the wireless LAN without the need to install any driver software. This is extremely useful for machines with limited driver support, e.g. Apple Macintosh machines and Linux machines.
- **Parallel Broadband**  
This unique feature allows bandwidth aggregation and fail-over redundancy capability when set to gateway mode which uses wireless distribution system to wirelessly link all associated access point gateway together.
- **Universal Configuration Software**  
Netkrom uConfig software allows users to get onto the web based configuration interface of AIR-BR500G/GH without the need to further manipulate the TCP/IP setup of the workstation.
- **Web-based Management Interface**  
Embedded with a HTTP server allows the configuration of the NETKROM AIR-BR500G/GH features via a user friendly web-based management interface. In addition, firmware upgrade can be done through this interface as well.
- **IEEE 802.1x Authentication and Wi-Fi Protected Access (WPA)**  
Netkrom AIR-BR500G/GH supports latest wireless security Wi-Fi Protected Access (WPA) using both Pre-Share Key and 802.1x EAP authentication. A wide range of IEEE 802.1x authentication methods like EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP for strong mutual authentication and data encryption is supported.
- **Wireless Pseudo Virtual LAN**  
Allows the creation of wireless virtual nodes or workgroups for wireless clients to increase the privacy in a wireless LAN installation.
- **SNMP**  
For easy remote management and monitoring of the Netkrom AIR-BR500G/GH through standard SNMP software.



- **STP**

Spanning-Tree Protocol provides path redundancy while preventing undesirable loops in the network. It forces certain redundant data paths into a standby (blocked) state. If one network segment in the Spanning-Tree Protocol becomes unreachable, or if Spanning-Tree Protocol costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and re-establishes the link by activating the standby path.

### **1.3    NETKROM AIR-BR500G/GH Package**

NETKROM AIR-BR500G/GH retail package contains the following items:

- 1 x Netkrom AIR-BR500G/GH
- 1 x Power over Ethernet Injector
- 1 x 110-220v Power Supply
- 1 x Product CD (including Quick Install Guide, User's Manual, Firmware Recovery Tool & Utilities)

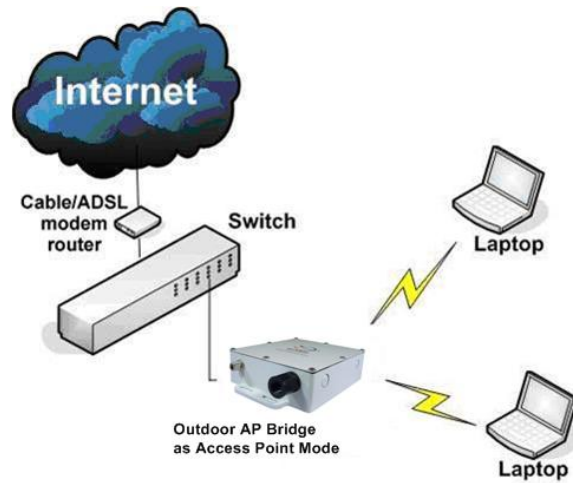
### **1.4    When to use which mode**

Netkrom AIR-BR500G/GH is unique in the sense that it may operate in up to 5 different netkrom modes in order to best suit any type of network application that you require.

This section presents a brief outline of the different network applications that can be accommodated through the different modes of Netkrom AIR-BR500G/GH.

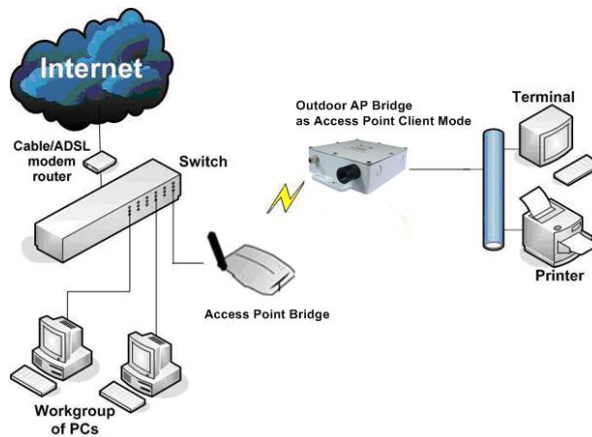
### 1.4.1 The Access Point Mode

This is the default mode of Netkrom AIR-BR500G/GH. The **Access Point** mode enables you to bridge wireless clients to the wired network infrastructure.



### 1.4.2 The Access Point Client Mode

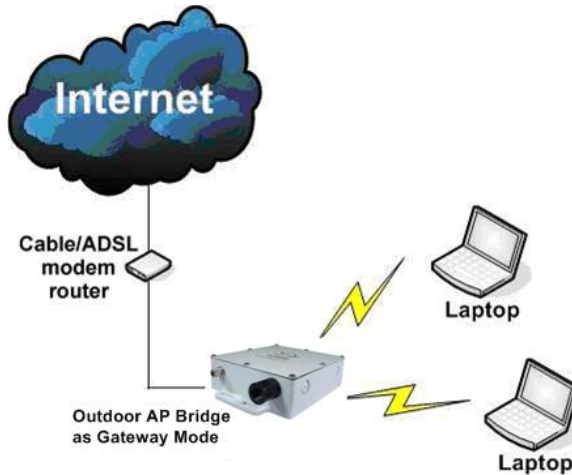
In **Access Point Client** mode, Netkrom AIR-BR500G/GH acts as a wireless client which can operate wirelessly with another access point to perform transparent bridging between two Fast Ethernet networks.



### 1.4.3      The Gateway Mode

Or put it more simply, Broadband Internet sharing in a wireless network!

Since Netkrom AIR-BR500G/GH supports several types of broadband connections, the first step in setting up Netkrom AIR-BR500G/GH as a *Broadband Internet Gateway* is to identify the type of broadband Internet access you are subscribed to.



#### **Static IP address**

Use this type of connection if you have subscribed to a fixed IP address or to a range of fixed IP addresses from your Internet Service Provider.

#### **Dynamic IP address**

When powered using this type of connection, Netkrom AIR-BR500G/GH requests for an IP address which will be automatically assigned to it by your Internet Service Provider.

This type of connection applies for instance, to:

- Cable Vision subscribers
- @HOME Cable Service users

#### **PPP over Ethernet (PPPoE)**

Select this type of connection if you are using ADSL services in a country utilising standard PPP over Ethernet for authentication.

For instance:

If you are in Germany which uses T-1 connection or

If you are using SingNet Broadband or Pacific Internet Broadband in Singapore.

### **Singapore ADSL (Ethernet 512K)**

This applies to ADSL subscribers in Singapore including SingTel Magix SuperSurf users.

### **Australia BPA Cable**

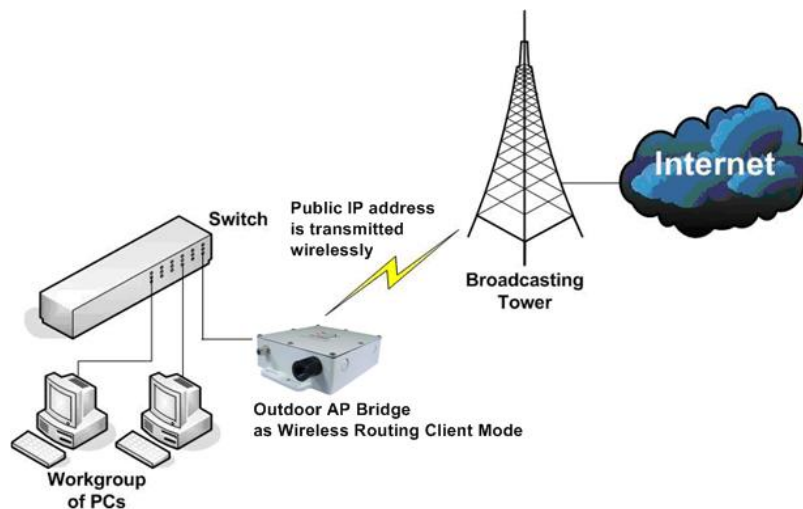
This connection type is customised for Big Pond Cable Internet users in Australia.

### **PPTP**

The Point-to-Point Tunnelling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.

#### **1.4.4      The Wireless Routing Client Mode**

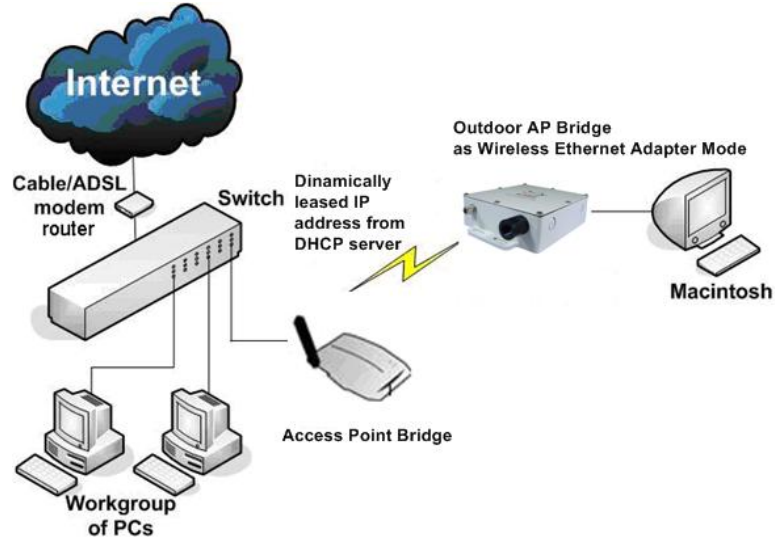
An application of this mode would be for the Ethernet port of the **Wireless Routing Client** to be used for connection with other devices on the network while accessing to the Internet would be achieved through wireless communication with wireless ISP.



### 1.4.5      Wireless Ethernet Adapter Mode

Similarly to the Access Point Client mode, Netkrom AIR-BR500G/GH used in this mode, is able to communicate wirelessly with another access point to perform transparent bridging between two networks.

However here, the **Wireless Ethernet Adapter** connects a single wired workstation only. No client software or drivers are required while using this mode.



### 1.4.6      The Wireless Bridge Link Mode

The **Wireless Bridge Link** mode allows point-to-point communication between different buildings. It enables you to bridge wireless clients that are kilometres apart ( eg. within 100 metres between two buildings ) while unifying the networks. In this scenario, you may configure two Netkrom AIR-BR500G/GH units to perform transparent bridging between two buildings.

## **2.1    Setup Requirements**

Before starting, please verify that the following is available:

- CAT5/5e networking cable
- At least one computer is installed with a Web browser and a wired or wireless network interface adapter
- TCP/IP protocol is installed and IP address parameters are properly configured on all your network's nodes

## **2.2    Netkrom AIR-BR500G/GH Hardware Installation**

In three simple steps, you may power ON and begin configuring Netkrom AIR-BR500G/GH.

1. You can choose to connect the external antenna to the N connector of Netkrom AIR-BR500G/GH
2. Use the Ethernet cable to connect your PC to the socket labelled LAN on Netkrom AIR-BR500G/GH.
3. Attach the power adapter to the main electrical supply, and connect the power plug onto the socket on power over Ethernet injector.

You may turn the device ON.

**Chapter 3 Access to Web-based Interface**

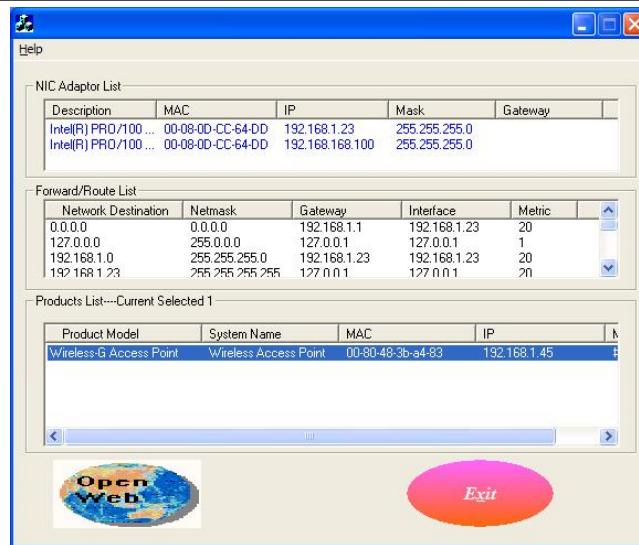
There are two methods to access to the web-based Interface of Netkrom AIR-BR500G/GH:

- **Through our Netkrom AIR-BR500G/GH Utility – uConfig**  
You can access to the web-based interface directly without the need to assign an IP address to your PC.
- **Enter IP address of Netkrom AIR-BR500G/GH in the address bar of Internet Explorer**  
You need to assign an IP address to your PC, such as 192.168.168.xxx, where x can take any value from 2 to 254, so that it is in the same subnet as Netkrom AIR-BR500G/GH.

### 3.1 Access to the Web interface with uConfig

Netkrom has developed a powerful uConfig utility which will provide you hassle-free access to the web-based configuration page. It has been designed to give you direct access to the Web interface.

4. Insert the Product CD into your CD-ROM drive. The CD will run automatically.
5. From the **Utilities** section, select to install the **uConfig** utility to your hard disk.
6. When the utility has been installed, double-click on the **uConfig** icon.



7. Select Netkrom *AIR-BR500G/GH* in the **Products List** section and click on **Open Web** button.
8. At the login page, press the **Log On!** button to enter the configuration page.

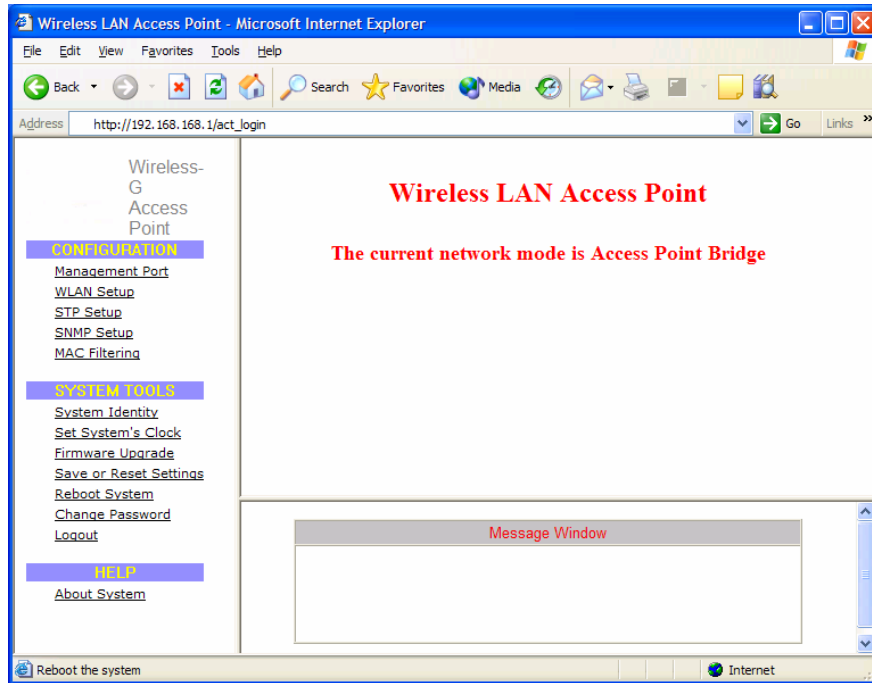
### Wireless LAN Access Point Management

Please enter your password:

(Forgot your password? - see the User's Guide for instructions.)

9. You will then reach the home page of Netkrom *AIR-BR500G/GH*'s web-based interface.





### 3.2 Verify the IP address of Netkrom AIR-BR500G/GH- The NpFind Utility

Netkrom has designed another utility program **NpFind**, intended to help you verify the IP address of your Netkrom product.

Follow the next steps to check the IP address of your Netkrom AIR-BR500G/GH.

1. Insert the Product CD into the CD-ROM drive.
2. It will automatically run to the page shown below.
3. Click on **Utilities**.
4. Click on the **NpFind** program to run it.

The screen will automatically display the IP address of the Netkrom device detected.



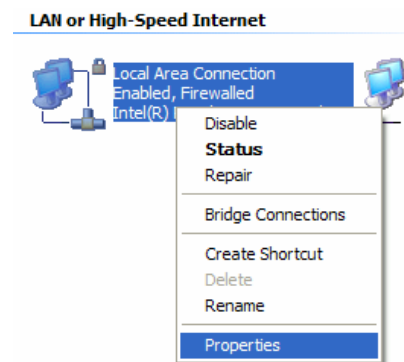
### 3.3 Direct access to web-based interface via Internet Explorer

For this method, you need to assign an IP address to your PC so that it belongs to the same subnet as your Netkrom AIR-BR500G/GH. In this example, we are using Windows XP for illustration, for Windows 98/98SE/2000/NT/ME, kindly refer to **Appendix III “TCP/IP Configuration”**.

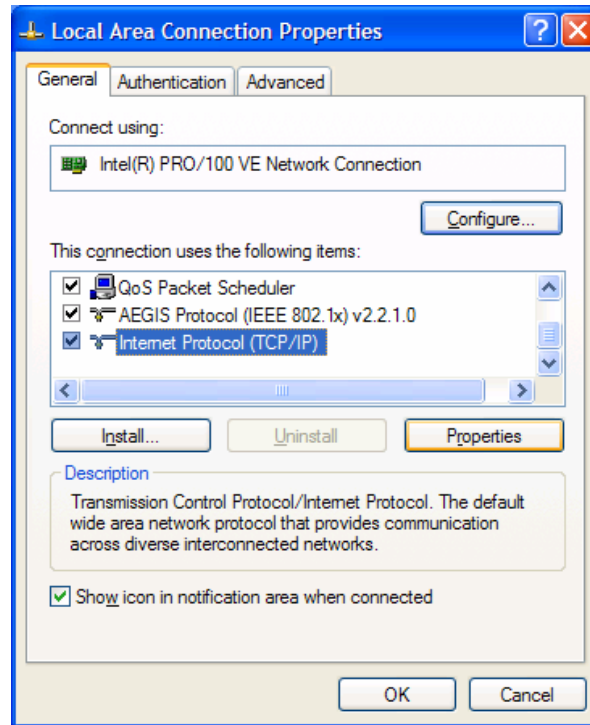
1. Go to your desktop, right click on **My Network Places** and select **Properties**.



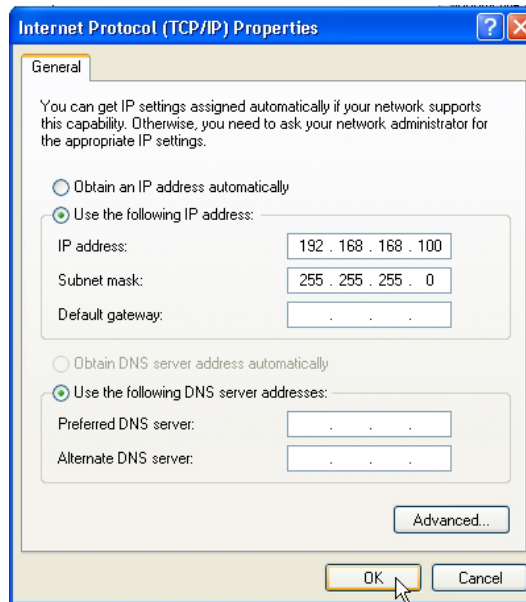
2. Right click on your Ethernet adapter and select **Properties**.



3. Next, select on **Internet Protocol (TCP/IP)** and click on **Properties** button.



4. Since the default IP address for your Netkrom AIR-BR500G/GH is 192.168.168.1, we need to set your PC's IP address to be the same subnet as your access point. Therefore, in this example, we assign an IP address of *192.168.168.100* and subnet mask as *255.255.255.0*.



5. Click **OK** button to update the changes.
6. Now, you may open the MS-DOS prompt window and type in *ping 192.168.168.1* to verify whether your PC can communicate with Netkrom AIR-BR500G/GH.
7. If your TCP/IP settings are correct, you will get replies to the ping command:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>ping 192.168.168.1

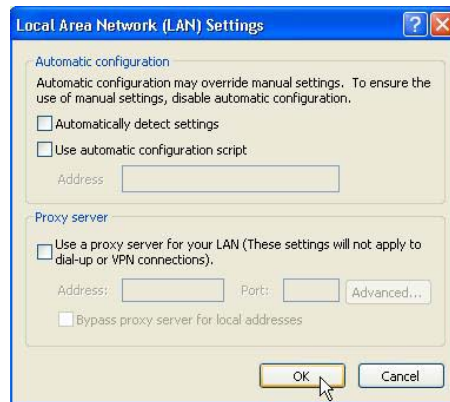
Pinging 192.168.168.1 with 32 bytes of data:
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64
Reply from 192.168.168.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.168.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

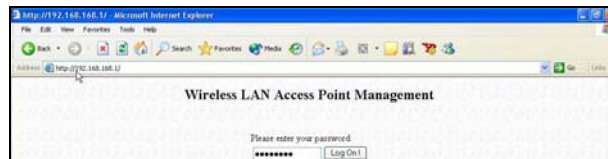
8. Launch your Web browser. Under the **Tools** tab, select **Internet Options**.



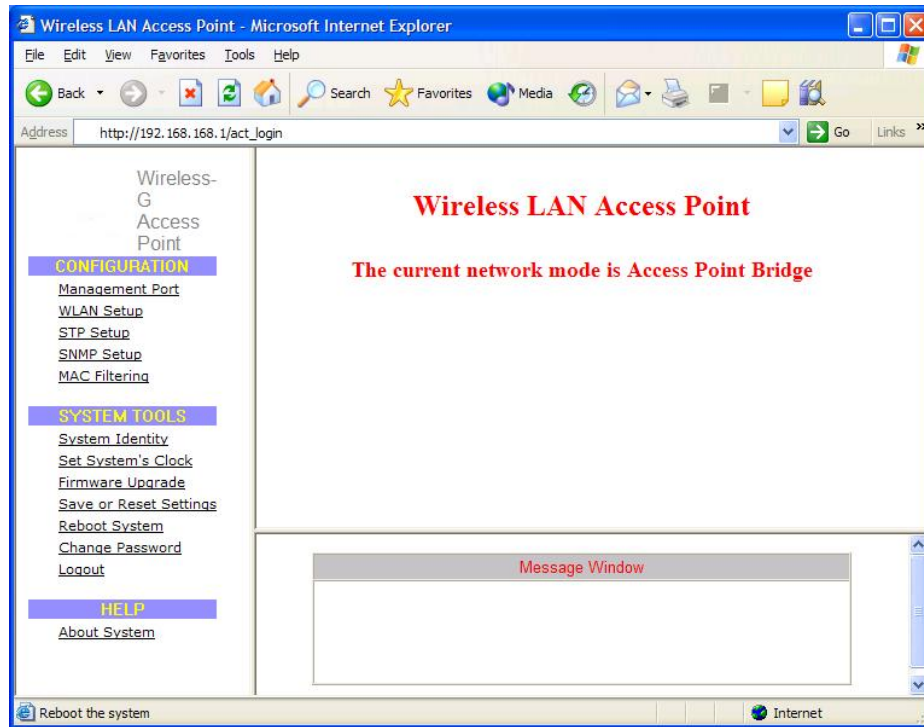
9. Open the **Connections** tab and in the **LAN Settings** section, disable all the option boxes. Click **OK** button to update the changes.



10. At the **Address** bar, enter **http://192.168.168.1** and press **Enter** from your keyboard.
11. At the login page, click the **Log On!** button to enter the configuration pages.



12. You will then reach the home page of Netkrom AIR-BR500G/GH's Web interface.



### Chapter 4 Common Configuration

This chapter illustrates the following features, which are available in ALL the operating modes of Netkrom AIR-BR500G/GH, unless stated otherwise.

- **Management Port**
- **WLAN Setup**
- **WLAN Security**
- **SNMP Setup**

#### 4.1 Management Port Setup

This section shows you how to customize the parameters of Netkrom AIR-BR500G/GH to suit the needs of your network. It also explains how to make use of the built-in DHCP server of Netkrom AIR-BR500G/GH.

##### Setting up your LAN

You can opt to adjust the default values of Netkrom AIR-BR500G/GH and customize them to your network settings.

**LAN SETUP**

Click on **Management Port** from the **CONFIGURATION** menu.

In the **Management Port Setup** page, refer to the table below to replace the default settings of Netkrom AIR-BR500G/GH with appropriate values to suit the needs of your network.

IP Address	192	168	168	1
Network Mask	255	255	255	0
Management Gateway Ip	0	0	0	0
DHCP Start IP Address	192	168	168	100
DHCP End IP Address	192	168	168	254
DHCP Gateway IP Address	0	0	0	0
<input type="checkbox"/> Always use these DNS servers:				
Primary DNS IP Address	0	0	0	0
Secondary DNS IP Address	0	0	0	0
DHCP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			

**Apply** **Help**

Click on **Apply** to save your new parameters.



## Chapter 4 Common Configuration

This table describes the parameters that can be modified in the **Management Port Setup** page.

Parameters	Description
<b>IP Address</b>	The IP address of Netkrom AIR-BR500G/GH is set by default to <b>192.168.168.1</b> .
<b>Network Mask</b>	The Network Mask serves to identify the subnet in which Netkrom AIR-BR500G/GH resides. The default network mask is <b>255.255.255.0</b> .
<b>DHCP Start IP Address</b>	This is the first IP address that the DHCP server will assign. The value that you input here should belong to the same subnet as Netkrom AIR-BR500G/GH. For example, if the IP address and network mask of your Netkrom AIR-BR500G/GH are 192.168.168.1 and 255.255.255.0 respectively, the DHCP Start IP Address should be 192.168.168.X, where X can take any value from 2 to 254. This value is pre-set to <b>192.168.168.100</b> .
<b>DHCP End IP Address</b>	This is the last IP address that the DHCP server can assign. It should also belong to the same subnet as Netkrom AIR-BR500G/GH. For instance, if the IP address and network mask of your Netkrom AIR-BR500G/GH are 192.168.168.1 and 255.255.255.0 respectively, the DHCP End IP Address should be 192.168.168.X, where X can take any value from 2 to 254. It is pre-set as <b>192.168.168.254</b> .
<b>DHCP Gateway IP Address</b>	Inserting a DHCP gateway IP address will enable the DHCP server to automatically assign an IP address to any PC belonging to a different subnet or LAN.
<b>Always use these DNS servers</b>	If this checkbox is enabled, the DHCP server will also resolve the DNS queries of the computers. Otherwise, you will have to set up DNS information manually for every PC in your network.
<b>Primary DNS IP Address</b>	Your ISP usually provides the IP address of the DNS server.
<b>Secondary DNS IP Address</b>	This optional field is reserved for the IP address of a secondary DNS server.
<b>DHCP Server</b>	If you disable the DHCP server, you will need to manually configure the TCP/IP parameters of each PC in your network.

### 4.1.1 To view the active DHCP leases

The following will guide you to a page display of the active IP address leases that have been allocated by the built-in DHCP server of Netkrom AIR-BR500G/GH.

**View Active DHCP Leases**

Click on **Management Port** from the **CONFIGURATION** menu.

Go to the **Advanced DHCP Server Options** section, click on the **Show Active DHCP leases** button.

Advanced DHCP Server Options

Show Active Dhcp Leases

Dhcp Server Reservations

The **DHCP Active Leases** table displays:

- The **IP Address** that has been allocated to the DHCP client
- The **Host Name** of the DHCP client
- Its **Hardware (MAC) Address**
- The date and time at which the IP address leased **expires**

DHCP Active Leases

IP Address	Host Name	Hardware Address	Expires
------------	-----------	------------------	---------



#### NOTE

Invalid date and time displayed in the Expires column indicates that the clock of your Netkrom AIR-BR500G/GH has not been properly set. Please refer to the **SYSTEM TOOLS** section for more details on how to set the system clock.

### 4.1.2 To reserve specific IP addresses for predetermined DHCP clients

Making an IP address reservation lets you inform the DHCP server to exclude that specific address from the pool of free IP addresses it draws on for dynamic IP address allocation.

For instance, if you set up a publicly accessible FTP/HTTP server within your private LAN, while that server would require a fixed IP address, you would still want the DHCP server to dynamically allocate IP addresses to the rest of the PCs on the LAN.

The following shows you how to reserve a particular IP address.

**Reserve Specific IP addresses**

Click on **Management Port** from the **CONFIGURATION** menu.

Go to the Advanced DHCP Server Options section, click on the **DHCP Server Reservations** button.

**Advanced DHCP Server Options**

Fill in:  
The host portion of the **IP Address** to reserve.  
The **Host Name**, if there is any, else, leave it blank.  
The **Hardware Address**, in pairs of two hex values

**DHCP Server Reservations**

IP Address	Host Name	Hardware Address
------------	-----------	------------------

IP Address: 192.168.168.120 Host Name: Compex

Hardware Address: 08 20 e2 14 1d 2a

Click on **Add** button.

### Reserve Specific IP addresses (continued...)

Press the **Apply** button to make your new entry effective.

The **DHCP Reservations** page will then be refreshed to illustrate the currently reserved IP addresses.

If you do not need the DHCP server to reserve an IP address anymore, you can delete the DHCP Server Reservation thus:



### Delete DHCP Server Reservation

Select the reserved IP address to delete.

Click on **Delete**.

The **DHCP Server Reservations** table will then be refreshed to reflect your changes.





### NOTE

- When creating a DHCP reservation, you can opt to key in either the Host Name or the Hardware Address of the DHCP client.
- If you have entered both, the DHCP server will first check the hardware address.

If a match in hardware address has been found, the Host Name will then be ignored.

---

### 4.2 WLAN Setup

This section shows how to perform the following functions:

**Basic:**

This function performs a basic setup of the wireless modes of operation.

**Security:**

This function performs data encryption and protection for the router.

**Advanced:**

This function furthers the basic configuration of the router by setting the system's additional parameters such as Access Control, WDS, WMM and Long Distance Parameters.

**Statistics:**

This function uses the **Scan Feature** to monitor and interpret the statistics data collected.

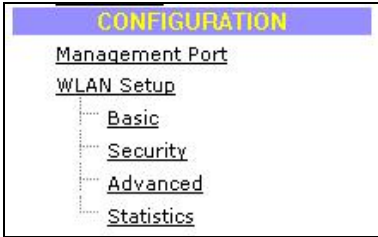
It also covers the **Show Link Information** option featured ONLY in **wireless client mode**.

#### 4.2.1 To configure the Basic setup of the wireless mode

The following will guide you to configure the basic setup of the wireless mode you have selected.

**Basic Setup Wireless Mode**

Double-click on **WLAN Setup** from the **CONFIGURATION** menu. You will see the sub-menus expanded under **WLAN Setup**. Click on **Basic**.



The default operating mode of Netkrom AIR-BR500G/GH is the **Access Point** mode.

Make your selection from

the **Network Mode** drop-down list.

Click on the **Apply** button to access the setup page of your selected mode.

NetWork Mode Setup

NetWork Mode: Access Point (selected)

Note: NetMode switched will

Apply

### Basic Setup Wireless Mode (continued...)

In the Mode **Setup** page:

Access Point Setup

The Current Mode: Access Point (Change)

Access Point Name: Wireless-G Access Point

ESSID: Wireless-G

Wireless Profile: 802.11b/g mixed

Country: UNITED STATES (Edit Country Setting)

Channel: SmartSelect (Channel Survey)

Tx Rate: Fully Auto

Closed System: Disable

Note: Changes made will only take effect after rebooting.

The Access Point Name field appears when Netkrom AIR-BR500G/GH is in AP/Gateway mode and refers to the identity of the device.

Access Point Name: Wireless-AG Access Point

In AP/Gateway mode, the ESSID uniquely identifies each WLAN.

ESSID: netkrom

The **Wireless Profile** drop-down list provides a selection of network environment types in which to operate Netkrom AIR-BR500G/GH:

Wireless Profile: 802.11b/g mixed

Country: 802.11a

Channel: 802.11b/g mixed

Tx Rate: 802.11g only

## Chapter 4 Common Configuration

---

- 802.11a;
- 802.11b only;
- 802.11b/g mixed, when both b and g clients are present;
- 802.11g only

Country	UNITED STATES	Edit Country Setting
---------	---------------	----------------------

Choose a **Country** that you are located.  
Click on the **Edit Country Setting** button  
to select your country.

Click on the **Apply** button to update the  
changes.

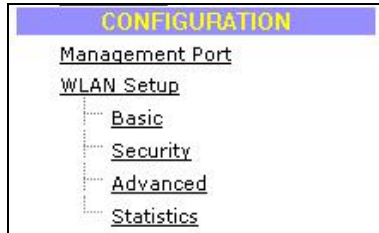


### 4.2.2 To configure the Advanced setup of the wireless mode

The following will guide you to configure the advanced setup of the wireless mode you have selected.

#### Advanced Setup Wireless Mode

Double-click on **WLAN Setup** from the **CONFIGURATION** menu to expand into the four sub-menus. From here, click on **Advanced**.



In the **WLAN Advanced Setup** page:

A screenshot of the 'WLAN Advanced Setup' configuration page. The page contains several settings with input fields and dropdown menus:

- Beacon Interval: 100 (range 100:20-1000)
- Data Beacon Rate (DTIM): 1 (range 1:1-16384)
- RTS/CTS Threshold: 2346 (range 2346:256-2346)
- Frag Threshold: 2346 (range 2346:256-2346)
- Transmit Power: Maximum (dropdown menu)
- Radio Off When Ethernet No Link: Disable (dropdown menu)
- Auto Reboot Timer: 00:00 (range 00:00-23:59) and a Disable button

Below the settings, there is a note: "Note: Changes made will only take effect after rebooting." and two buttons: "Save" and "Reboot".

At the bottom, there is a section titled "Extended Features" with four buttons: "Access Control", "WDS Configuration", "WMM Parameters", and "Long Distance Parameters".

Setup Wireless Mode (continued...)				
<p>The <b>Beacon Interval</b> is the amount of time between beacon transmissions. A beacon is a guidance signal sent by the access point to announce its presence to other access points. It also sends information, such as timestamp, SSID, and other parameters regarding the access point to other access points that are within the specified range. The access point needs the beacon interval to know when to receive the beacon from the other access point.</p>	<table border="1"> <tr> <td>Beacon Interval</td> <td>100</td> <td>(100:20-1000)</td> </tr> </table>	Beacon Interval	100	(100:20-1000)
Beacon Interval	100	(100:20-1000)		
<p>The <b>Data Beacon Rate (DTIM)</b> determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set at 100, its default setting, and the data beacon rate is set at 1, its default setting, then the access point sends a beacon containing a DTIM every 100 Kμsecs. One Kμsec equals 1,024 microseconds.</p>	<table border="1"> <tr> <td>Data Beacon Rate (DTIM)</td> <td>1</td> <td>(1:1-16384)</td> </tr> </table>	Data Beacon Rate (DTIM)	1	(1:1-16384)
Data Beacon Rate (DTIM)	1	(1:1-16384)		
<p>The <b>RTS/CTS Threshold</b> value determines the minimum size of a packet in bytes that would trigger the RTS/CTS mechanism.</p>	<table border="1"> <tr> <td>RTS/CTS Threshold</td> <td>2346</td> <td>(2346:256-2346)</td> </tr> </table>	RTS/CTS Threshold	2346	(2346:256-2346)
RTS/CTS Threshold	2346	(2346:256-2346)		
<p>The <b>Frag Threshold</b> value indicates the maximum size that a packet can reach without being fragmented. This value ranges from 256 to 2346 bytes.</p>	<table border="1"> <tr> <td>Frag Threshold</td> <td>2346</td> <td>(2346:256-2346)</td> </tr> </table> <p>This value extends from 256 to 2346 bytes, where a value of 0 indicates that all the packets should be transmitted using RTS.</p>	Frag Threshold	2346	(2346:256-2346)
Frag Threshold	2346	(2346:256-2346)		
<p>The <b>Transmit Power</b> drop-down list lets you pick from a range of transmission power.</p>	<table border="1"> <tr> <td>Transmit Power</td> <td>Maximum</td> </tr> </table>	Transmit Power	Maximum	
Transmit Power	Maximum			
<p>Enabling <b>Radio Off When Ethernet No Link</b> option allows your AP to turn off the radio signal so that no wireless clients can connect to it. This might occur when your</p>	<p><b>In AP/Gateway mode ONLY:</b></p> <table border="1"> <tr> <td>Radio Off When Ethernet No Link</td> <td> <div>Disable</div> <div>Disable</div> <div>Enable</div> </td> </tr> </table>	Radio Off When Ethernet No Link	<div>Disable</div> <div>Disable</div> <div>Enable</div>	
Radio Off When Ethernet No Link	<div>Disable</div> <div>Disable</div> <div>Enable</div>			

Ethernet cable is disconnected to the network)

If this function is enabled, the wireless radio will be turned off if there is no Ethernet connection. The wireless radio will be turned back on when the Ethernet link is restored.

The turning ON or OFF delay takes about 60 seconds after detecting whether the Ethernet link is UP or DOWN respectively.

The **Auto Reboot Timer** is the time setting for the access point to automatically reboot.

Auto Reboot Timer	00:00	Disable ▼
-------------------	-------	-----------



### NOTE

The values illustrated in the examples are suggested values for their respective parameters.

---

### 4.3 Scan for Site Survey (For Wireless Client Mode Only)

This feature only available in **wireless client mode** (**Access Point Client**, **Wireless Routing Client** and **Wireless Ethernet Adapter**).

- When a Netkrom AIR-BR500G/GH is connected to wired network and a set of wireless stations, it is referred to as a **Basic Service Set (BSS)**. The MAC address of Netkrom AIR-BR500G/GH is used as entry here.
- **SSID** refers to the network name which uniquely identifies the network to which Netkrom AIR-BR500G/GH is connected.
- **Chan** refers to the channel being used for transmission.
- **Auth** refers to the types of authentication, such as WPA, WPA-PSK, etc being used by the access point.
- **Alg** refers to the types of algorithm, such as WEP, TKIP, etc being used by the access point.
- **Signal** describes the strength of the signal received in percentage.

**Scan For Site Survey**

In the Mode **Setup** page, click on the **Site Survey** button.

### AP Client Setup

The Current Mode	<b>Access Point Client</b>	<input type="button" value="Change"/>
Station Name	<input type="text" value="Wireless-AG Access Point"/>	
SSID	<input type="text" value="netkrom"/>	<input type="button" value="Site Survey"/>
Wireless Profile	<input type="button" value="802.11b/g mixed"/>	
Country	<input type="button" value="802.11a"/> <input type="button" value="802.11b only"/> <input type="button" value="802.11b/g mixed"/> <input type="button" value="802.11g only"/>	<input type="button" value="Edit Country Setting"/>
Tx Rate		

*Note: Changes made will only take effect after rebooting.*

### Scan For Site Survey (continued...)

The **Site Survey** provides a list of the **BSS** and **SSID** available, the **Chan** (channels), **Auth** (Authentication), **Alg** (Algorithm) being used, and the strength of the **Signal** received.

To configure to a different SSID:

Select the radio button corresponding to the SSID you want to configure to.

Click on the **Apply** button to effect the change and return to the Setup page.

Click on the **Refresh** button.

Site Survey					
BSS	SSID	Chan	Auth	Alg	Signal
<input type="radio"/> 000b6b37e955	Netkrom-arc-test	11	OPEN	NONE	13%
<input checked="" type="radio"/> 000b6b37ed6f	Netkrom-OpenBSD-Node	3	OPEN	NONE	28%
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>					

#### 4.3.1 Show Link Information (For Wireless Client Mode Only)

This function offers a summary of the link data when Netkrom AIR-BR500G/GH is in the **wireless client mode**, i.e., either of the *Access Point Client*, *Wireless Routing Client* or the *Wireless Ethernet Adapter* mode.

### Show Link Information

In the Mode **Setup** page, go to the **Link Information** section.

Link Information	
<input type="button" value="Show Link Information"/>	

Click on the **Show Link Information** button. When an access point is connected to a wired network and a set of wireless stations, it is referred to as a **Basic Service Set** (BSS).

The **Link Information** table illustrates the following data:

Link Information	
State	Associated BSS ID=00:80:48:2B:E3:27
Current Channel	1
Signal Strength	68%

**State** refers to the MAC address of the BSS.

**Current Channel** is the channel being presently used for transmission.

**Signal Strength**, given in percentage form, shows the intensity of the signal received and hence the connection strength.

### 4.4 Wireless Extended Features

The **Wireless Extended Features** are ONLY available when Netkrom AIR-BR500G/GH operates in all modes as tabulated below:

Features	Mode
Access Control	Access Point and Gateway
Wireless Distributed System (WDS)	Access Point and Gateway
WMM Parameters	All modes except for Wireless Bridge Link
Outdoor Parameters	All modes

#### 4.4.1 Access Control – The Wireless Pseudo VLAN

A **VLAN** is a group of PCs or other network resources that behave as if they were connected to a single network segment.

Those stations which are assigned to the same VLAN share network resources and bandwidth as if they were connected to the same segment. Conversely, only the stations within the same VLAN can access each other.

A **Wireless Pseudo VLAN** acts by segregating a single wireless LAN into multiple virtual LANs so that communication is possible only among wireless clients within the same VLAN.

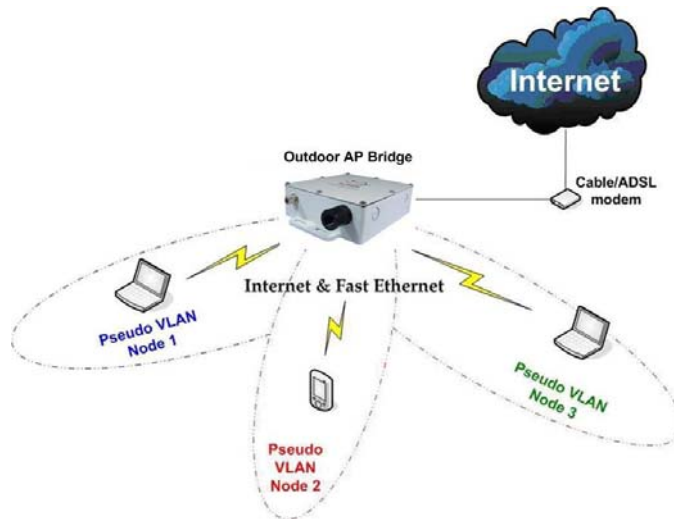
When operating in the **Gateway** mode, Netkrom AIR-BR500G/GH lets you create VLANs containing either a single user, and referred to as *Wireless Pseudo VLAN Per Node*, or a group of users, termed *Wireless Pseudo VLAN Per Group*.

When operating in the **Access Point** mode, Netkrom AIR-BR500G/GH allows you to define *Tag VLANs* in addition to the *Wireless Pseudo VLAN Per Node* and the *Wireless Pseudo VLAN Per Group*.

To learn more about Netkrom's exclusive **Wireless Pseudo VLAN**, please refer to the whitepaper available online at [www.netkrom.com](http://www.netkrom.com).

### 4.4.1.1 Wireless Pseudo VLAN Per Node

When implemented, this mode isolates each wireless client into its own pseudo VLAN. Wireless clients can therefore access resources on the wired network but are unable to see each other or access each other's data.



The following steps demonstrate how to set up a *Wireless Pseudo VLAN per Node*.

**Wireless Pseudo VLAN – Per Node**

From **WLAN Setup** under **Configuration**, click on **Advanced**, which shows the **WLAN Advanced Setup** page.

Go to the **Extended Features** section, and click on the **Access Control** button.

The **Wireless Pseudo VLAN** function is *Disabled* by default.

Select **Per Node** from the drop-down list.

Click on the **Apply** button.

**Extended Features**

Access Control

WDS Configuration

VMM Parameters

Long Distance Parameters

**Access Control Setup**

Disable

Disable

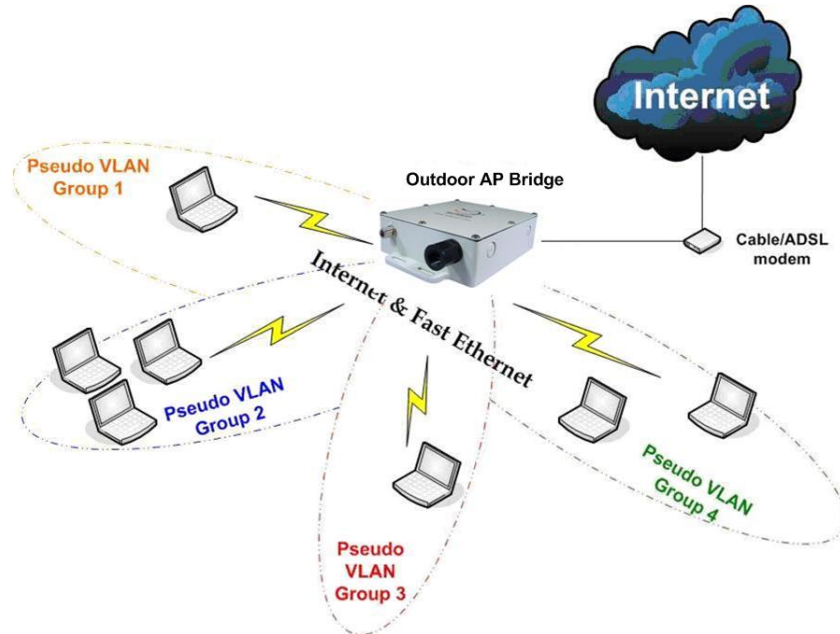
Per Node

Ad Pseudo VLAN

Tgg VLAN

### 4.4.1.2 Wireless Pseudo VLAN Per Group

Netkrom AIR-BR500G/GH can configure up to four 'groups' of wireless clients identified by their MAC address. Whenever a wireless client requests network access, Netkrom AIR-BR500G/GH will first verify whether its MAC address is present in any of the Pseudo VLAN groups. If it is, Netkrom AIR-BR500G/GH will grant it access to all the wired system resources and to all other wireless clients belonging to the same Pseudo VLAN group only.



The following steps demonstrate how to set up Wireless Pseudo VLAN Groups.

**Wireless Pseudo VLAN – Per Group**  
From **WLAN Setup** under **Configuration**, click on **Advanced**, which shows the **WLAN Advanced Setup** page.  
Click on the **Access Control** button.

Extended Features

Access Control

WMM Parameters

WDS Configuration

Long Distance Parameters



### Wireless Pseudo VLAN – Per Group (continued...)

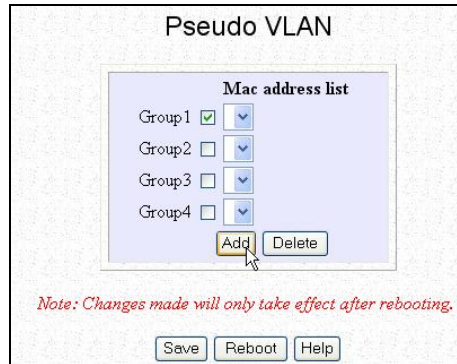
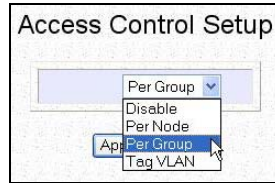
The **Wireless Pseudo VLAN** function is *Disabled* by default.

Select **Pseudo VLAN** from the drop-down list.

Click on the **Apply** button.

The **MAC Address List** enables you to manage specific VLAN groups by adding or deleting clients through their MAC address.

Click on the **Add** button.

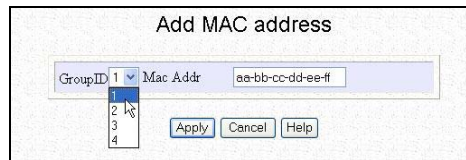


Select a group number from the **Group ID** drop-down list.

Fill in the **Mac Addr** field with the MAC address of the client in the format **xx:xx:xx:xx:xx** or **xx-xx-xx-xx-xx-xx**, where x is any value within the range 0-9 or a-f.

Click on the **Apply** button.

The updated **Mac Address List** page will appear as shown.



### Pseudo VLAN

#### Mac address list

Group1	<input checked="" type="checkbox"/>	aa-bb-cc-dd-ee-ff
Group2	<input type="checkbox"/>	
Group3	<input type="checkbox"/>	
Group4	<input type="checkbox"/>	

Add
Delete

*Note: Changes made will only take effect after rebooting.*

Save
Reboot
Help

### Delete client from a group

If you want to delete a particular client from a group:

Select the client to delete from the **Mac Address List**.

Click on the **Delete** button.

### Pseudo VLAN

#### Mac address list

Group1	<input checked="" type="checkbox"/>	11-22-33-44-55-66
Group2	<input type="checkbox"/>	11-22-33-44-55-66
Group3	<input type="checkbox"/>	aa-bb-cc-dd-ee-ff
Group4	<input type="checkbox"/>	

Add
Delete

*Note: Changes made will only take effect after rebooting.*

Save
Reboot
Help

This **Delete MAC Address** page will appear to confirm whether you want to delete the selected client.

If you do not want to delete the client:

Click on **Apply** button.

If you want to remove the client from the group:

Click on **Delete** button.

### Delete MAC address

GroupID: 1

Apply

Mac Addr: 11-22-33-44-55-66

Delete

### 4.4.1.3 Tag VLAN - [Available in Access Point mode ONLY]

While a port-based VLAN is limited in size since it can only exist within the confines of a single Ethernet switch, a Tag VLAN is designed to extend the wired VLAN to individual wireless clients.

Here, each VLAN is identified by a 'tag', which the switch associates with specific ports. The switch will then pass this tag information with every data packet transmitted. By using the same tag on each access point in the network, full client roaming can be implemented while complying with VLAN integrity.

**Wireless Pseudo VLAN – Tag VLAN**

From **WLAN Setup** under **Configuration**, click on **Advanced**, which shows the **WLAN Advanced Setup** page.:

Go to the **Extended Features** section.

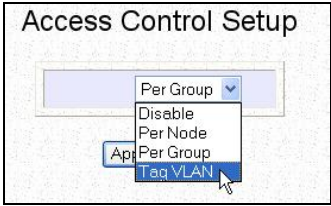

Click on the **Access Control** button.

The Wireless Pseudo VLAN function is *Disabled* by default.

Select Tag VLAN from the drop-down list.

Click on the **Apply** button.

The **Tag VLAN** page enables you to manage specific VLAN groups by adding or deleting clients through their MAC address.



Click on the **Add** button.

The 'Tag VLAN' window displays a table with two columns: 'VLAN ID' and 'Mac address list'. The table has five rows: Group1, Group2, Group3, Group4, and Guest domain. Each row has a checkbox and a dropdown menu. Group1 is selected, and its dropdown menu is open, showing '1'. Below the table are 'Add' and 'Delete' buttons. At the bottom of the window are 'Save', 'Reboot', and 'Help' buttons. A mouse cursor is pointing at the 'Add' button.

Select a group number from the **Group ID** drop-down list.

Fill in the **Mac Addr** field with the MAC address of the client in the format **xx:xx:xx:xx:xx** or **xx-xx-xx-xx-xx**, where x is any value between 0-9 or a-f.

Click on the **Apply** button.

The 'Add MAC address' dialog box shows a 'GroupID' dropdown menu with '1' selected. Next to it is a 'Mac Addr' text field containing 'aa-bb-cc-dd-ee-ff'. Below these are 'Apply', 'Cancel', and 'Help' buttons. A mouse cursor is pointing at the 'Apply' button.

The updated **Mac Address List** page will appear as shown on the right.

Repeat Step 4 if you need to add more clients or to configure more groups.

The 'Tag VLAN' window shows the updated state. The 'Mac address list' column now contains the MAC address 'aa-bb-cc-dd-ee-ff' for Group1. The 'Add' button is still visible, and a mouse cursor is pointing at the 'Save' button at the bottom.

### Delete client from a Tag VLAN

If you want to delete a particular client from a group:

Select the client to delete from the **Mac Address List**.

Click on the **Delete** button.

	VLAN ID	Mac address list
Group1 <input type="checkbox"/>	1	aa-bb-cc-dd-ee-ff
Group2 <input type="checkbox"/>	2	
Group3 <input type="checkbox"/>	3	
Group4 <input type="checkbox"/>	4	
Guest domain <input type="checkbox"/>	5	

Add Delete

Save Reboot Help

The **Delete MAC Address** page will appear to confirm whether you want to delete the selected client.

If you want to remove the client from the group:

Click on **Delete**.

Else click on **Apply**.

Click on the corresponding **Group** checkbox to enable a particular VLAN.

If you enable **Guest domain**, even those stations which are not identified in the **MAC address list** will still be allowed to access the Internet though they will not be able to communicate with each other

GroupID 1

Apply

Mac Addr e1-08-a2-bb-2e-f4

Delete

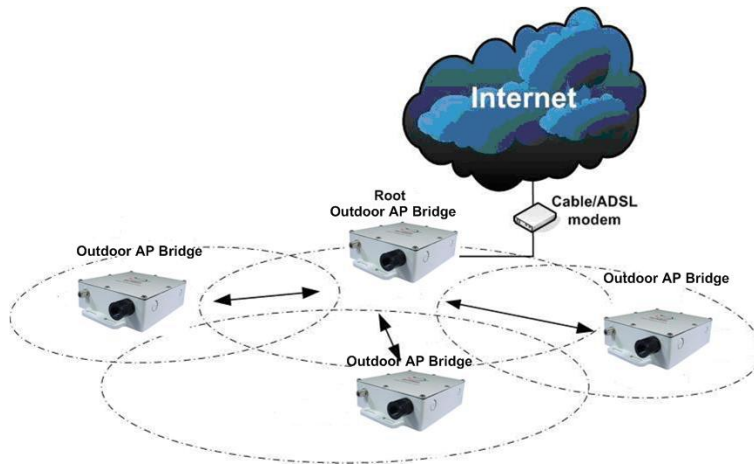
### 4.4.2 Wireless Setup - The Wireless Distributed System (WDS)

A distribution system links up several Netkrom AIR-BR500G/GH's and the areas they serve, creating a wider network in which mobile users can roam while still staying connected to the available network resources.

In a WDS, Netkrom AIR-BR500G/GH can drive a cell of wired and wireless clients while at the same time, connecting to other gateways. This requires the operational frequency channel to be the same within the cell controlled by your gateway as well as for its wireless links to the other gateways.

#### 4.4.2.1 Star Configuration WDS

In a star configuration WDS, links are established between one root Netkrom AIR-BR500G/GH and several satellite gateways positioned to increase the area covered.

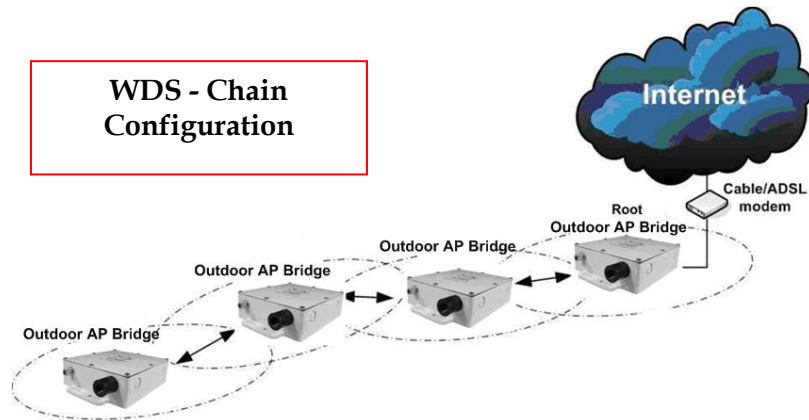


Here, the root gateway connects to the Internet and maintains three WDS links while each Outdoor AP Bridge gateway uses one port only for communication with the root.

### 4.4.2.2 Chain Configuration WDS

A chain configuration WDS spans an area in length, for instance a long corridor. Satellite access points are chained together starting from a root access point.

Netkrom AIR-BR500G/GH at either end of the chain will have only one WDS port enabled, while the access points in the middle will have two WDS ports configured to associate with the neighboring Netkrom AIR-BR500G/GH upward and downward in the chain.



The following steps will guide you in setting up WDS in your Netkrom AIR-BR500G/GH.

### WDS Configuration Setup

From **WLAN Setup** under **Configuration**, click on **Advanced** which shows the **WLAN Advanced Setup** page.

Go to the **Extended Features** section. Click on the **WDS Configuration** button.

As illustrated on the **WDS Setup**, the **WDS** feature is *Disabled* by default.


Select **Enable** from the **WDS Global Control** drop-down list to operate WDS.

Click on the **Apply** button.


At the **WDS Status** page:

Click on the **Add** button to expand your WDS.

### Extended Features

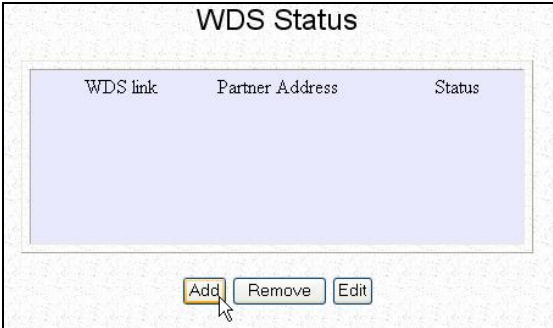


### WDS Setup



Please note that if you auto select your frequency channel (**SmartSelect**), you are not allowed to activate WDS Global Control.

### WDS Status





#### NOTE

To configure WDS, all your access points must be in the same channel; and both your access points at opposite WDS link must have each other's wireless MAC address



### WDS Configuration Setup (continued...)

On the **Add WDS Link** screen that appears:

Fill up the **Partner Address** field with the MAC address of the device to include in your WDS, using the format xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or a mix of: and -, and where x can take any hexadecimal value 0-9 or a-f.

Use the **Status** option to control whether you want to **Enable** this particular WDS link or to **Disable** it.

Click on the **Apply** button.

The **WDS Status** page will be updated as shown on the right.

If you want to modify the status entry for a WDS link:

WDS link	Partner Address	Status
1	11:22:33:44:55:66	Enable

Select the radio button on the left of that particular link as illustrated below left.

Click on the **Edit** button.

At the **Edit WDS Link** page which shows:

Select whether to enable or to disable the WDS link.

Click on the **Apply** button for the changes you made to take effect.

WDS Configuration Setup (continued...)

If you want to delete a WDS link:

Select the radio button on the left of that particular link.

Click on the **Remove** button.

An updated **WDS Status** page will be displayed.

WDS Status

WDS link	Partner Address	Status
<input checked="" type="radio"/> 1	<a href="#">11:22:33:44:55:66</a>	Enable
<input type="radio"/> 2	<a href="#">ab:cd:11:22:aa:ff</a>	Enable

Add Remove Edit

WDS Status

WDS link	Partner Address	Status
<input type="radio"/> 1	<a href="#">ab:cd:11:22:aa:ff</a>	Enable

Add Remove Edit

To view **WDS Statistics Info**:

Click on the hyperlink of the selected Partner Address.

The **Link ( Partner Address ) Statistics** table shown on the left will be displayed.

Click on the **Back** button to return to the **WDS Status** page.

WDS Status

WDS link	Partner Address	Status
<input type="radio"/> 1	<a href="#">11:22:33:44:55:66</a>	Enable

Add Remove Edit

Link(11:22:33:44:55:66) Statistics

State	Power Save					
joined	off					
Encryption	Advertised Cipher	Unicast Cipher	Multicast Cipher			
yes	None	None	None			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	0	0	0
Transmit	0	0	0	0	0	0
	Signal Strength (RSSI)			Data Rate (Mbps)		
Receive	295			1		
Transmit	2			1   1		
Receive Errors	Discarded Frames	Duplicate Frames	CRC Errors	Decrypt Errors	PHY Errors	DMA Errors
0	0	0	0	0	0	0
Transmit	Discarded	Excessive	DMA			



### NOTE

- If **WDS Global Control** is Disabled, every WDS link will be closed regardless of its status.

When **WDS Global Control** is set to Enabled, the status of every WDS link that you want to include still needs to be individually Enabled.

- In the WDS Statistics table, each entry corresponds to a particular WDS link.
- Although the WDS nodes may belong to different SSIDs, they MUST be configured in the same channel and use the same WEP keys (if the encryption feature is enabled) to be able to communicate with one another.

If the WDS-enabled access points are required to support too many operational wireless clients, you may find end-to-end throughput to be low (depending on the applications). For instance, end-to-end latency may become an issue in a very long WDS chain configuration.

---

### 4.4.3 WMM Parameters (available in all modes except for Wireless Bridge Link)


WMM stands for **Wireless Multi-Media**. WMM is a QoS (Quality of Service ) standard in IEEE 802.11E that we can adopt to improve and support the voice, video and multimedia applications. QoS can be realized through 4 different Access Categories (AC). Each AC type consists of an independent transmit queue and a channel access function with its own parameters that include Cwmin,Cwmax, AIFS, TxopLimit, ACM and Ack-policy.

The following steps demonstrate how to configure these WMM Parameters.

**WMM Parameters**

From **WLAN Setup** under **Configuration**, click on **Advanced**, which shows the **WLAN Advanced Setup** page.


Go to the **Extended Features** section, and click on the **WMM Parameters** button.

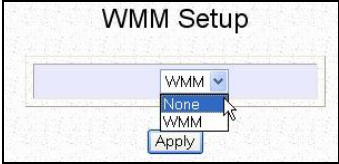
**Extended Features**  


The **WMM Setup** function is *WMM* by default.

Select **WMM** from the drop-down list

Click on the **Apply** button.

**WMM Setup**  


**WMM Setup**  


### AP WMM Parameters

AC TYPE	CWMin	CWMax	AIFS	TxopLimit	ACM	Ack-policy
AC_BE(0)	4	6	3	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI(2)	3	4	1	3008	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO(3)	2	3	1	1504	<input type="checkbox"/>	<input type="checkbox"/>

### BSS WMM Parameters

AC TYPE	CWMin	CWMax	AIFS	TxopLimit	ACM
AC_BE(0)	4	10	3	0	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	<input type="checkbox"/>
AC_VI(2)	3	4	2	3008	<input type="checkbox"/>
AC_VO(3)	2	3	2	1504	<input type="checkbox"/>

Note: Changes made will only take effect after rebooting.

Depending on the mode you set up, you have to select either AP (Access Point) or BSS (Basic Service Set) WMM Parameters. For instance, if the mode is AP, select AP WMM Parameters. The following parameters are described :

**CWmin** : It is the minimum Contention Window. It is a random number drawn from this interval or window for the backoff mechanism.

**CWmax** : It is the maximum Contention Window. It is a random number drawn from this interval or window for the backoff mechanism.

**AIFS** : Arbitrary Inter-frame Space. It is the minimum time interval between the wireless medium becoming idle and the start of transmission of a frame.

**TXOP Limit** : Transmission Opportunity. It is the minimum duration for which a QSTA can transmit after obtaining a TXOP.

**ACM** : Admission Control Management.

**Ack Policy**: Acknowledge Policy

### 4.4.4 Long Distance Parameters (available in all modes)

These parameters determine the distance between wireless clients to ensure that the wireless point-to-point communication takes place efficiently and effortlessly.

The following steps demonstrate how to configure these Long Distance Parameters.

#### Long Distance Parameters

From **WLAN Setup** under **Configuration**, click on **Advanced**, which shows the **WLAN Advanced Setup** page.

Go to the **Extended Features** section, and click on the **Long Distance Parameters** button.

The **Long Distance Parameters** function is *Disable* by default.

Select **Enable** from the drop-down list

Click on the **Apply** button.

To copy the reference data, click on **Show Reference Data**.

#### Extended Features

Access Control    WDS Configuration  
WMM Parameters    Long Distance Parameters

#### Long Distance Parameters

Outdoor: **Enable**  
Distance(meter): 100  
SlotTime(us): 9  
ACKTimeOut(us): 18  
CTSTimeOut(us): 18

Show Reference Data

Note: Enter the distance of the client from the AP, a set for recommended parameters for SlotTime, ACKTimeOut and CTSTimeOut will be computed. You can use the recommended parameters or make your own fine tunings. Changes made will only take effect after rebooting.

Save    Reboot

#### Long Distance Parameters

Outdoor: **Enable**  
Distance(meter): 100  
Show Reference Data

Microsoft Internet Explorer

Recommended slottime: 10 ;acknowdege timeout: 23; cts timeout:23

OK

Note: parameters for SlotTime, ACKTimeOut and CTSTimeOut will be computed. You

The parameters are described below:

**Outdoor:**

The Outdoor parameter is disabled by default. If set to Enable, the Outdoor parameters will be configured for outdoor communication over short or long distances specified.

**Distance:**

This parameter determines the distance between different buildings. It should be entered in meters.

**Slot Time:**

This parameter determines the slot time allocated by each wireless client ( that is, the sending and the receiving clients) to initiate and/or receive data transmission.

**ACK Timeout:**

This parameter determines the timeout allowed for the sending client to receive the acknowledgment response from the receiving client.

**CTS Timeout:**

This Clear-to-Send time is the one in which the wireless clients are ready to initiate and/or receive data transmission within a specified timeout.

### 4.5 WLAN Security

This section illustrates how to make your WLAN more secure. All the nodes in your network **MUST** share the same wireless settings to be able to communicate.

We will illustrate how to configure each type of security mode individually

To start with, follow the common preliminary steps described below to select the most appropriate security approach for protecting your wireless communications.

**Selecting Security Mode**

Click on **WLAN Setup** from the **CONFIGURATION** menu to select **Security**.

**WLAN Setup**

- Basic
- Security**
- Advanced
- Statistics

Make a selection from the **Security Mode** drop down menu.

The **Security Mode** is set to **NONE** by default.

Click on **Apply**.

**WLAN Security Setup**

Security Mode

NONE

NONE

WEP

WPA-PSK

802.1X

WPA-EAP

WPA2-PSK

WPA2-EAP

WPA-PSK-AUTO

WPA-EAP-AUTO

Apply



### 4.5.1 How to set up WEP [Available in ALL modes]

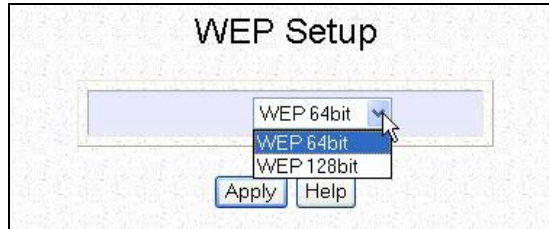
The guidelines below will help you to set up Netkrom AIR-BR500G/GH for using WEP.

#### Security Mode -WEP

At the **WEP Setup** page:

Select whether to use WEP 64bit or WEP 128 bit.

Click on **Apply**.



Netkrom AIR-BR500G/GH lets you define up to four different WEP keys.

Specify the key entry format, by selecting either:

- Use Alphanumeric Characters
- Use Hexadecimal

Enter your WEP keys in the **Key** fields.

#### Security Mode –WEP (continued...)

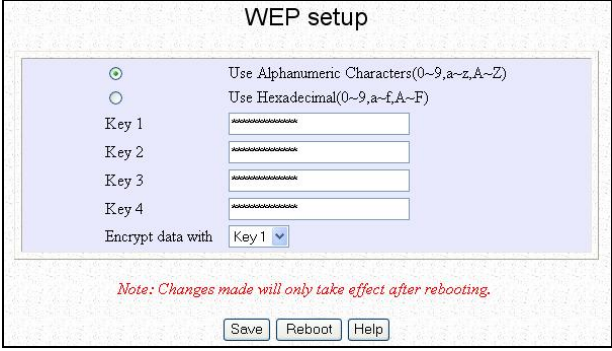
##### **When using 64-bit encryption:**

Your WEP key has to be either **5** alphanumeric characters or **10** hex characters long.



### **When using 128-bit encryption:**

Your WEP key has to be either **13** alphanumeric characters or **26** hex characters long.



The image shows a 'WEK setup' window with a light blue background. At the top, there are two radio buttons: the first is selected and labeled 'Use Alphanumeric Characters(0~9,a~z,A~Z)', and the second is labeled 'Use Hexadecimal(0~9,a~f,A~F)'. Below these are four text input fields labeled 'Key 1', 'Key 2', 'Key 3', and 'Key 4', each containing a series of asterisks. Below the keys is a dropdown menu labeled 'Encrypt data with' with 'Key 1' selected. At the bottom, there is a red italicized note: 'Note: Changes made will only take effect after rebooting.' and three buttons: 'Save', 'Reboot', and 'Help'.

Select which of the keys defined to **Encrypt data with**.

Click on **Save** and **Reboot** your Netkrom AIR-BR500G/GH.

A **Hexadecimal** value can only take in numbers **0-9** and letters **A-F** and is NOT case-sensitive.

### 4.5.2 How to set up WPA-PSK [Available in AP/Gateway mode ONLY]

The guidelines below will help you to set up Netkrom AIR-BR500G/GH for using WPA-PSK. (Please take note that the **WPA-PSK**, **WPA2-PSK** and **WPA-PSK-AUTO** security modes share the same functions).

#### Security Mode –WPA-PSK, WPA2-PSK, WPA-PSK-AUTO

At the **WLAN Security Setup** page:

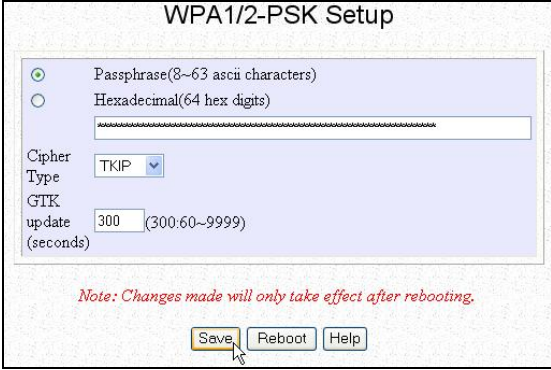
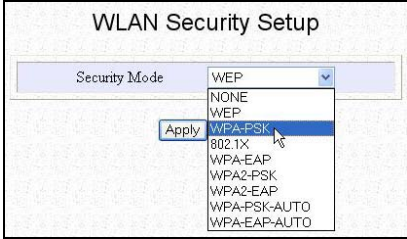
Select **WPA-PSK** mode.

Click on **Apply** button.

Specify the key entry format by selecting either:

- Passphrase (Alphanumeric characters)
- Hexadecimal

Fill in the pre-shared network key.



If you are using the **Passphrase** format, your entry can consist of a minimum of 8 alphanumeric characters or a maximum of 63 alphanumeric characters.

Otherwise, when using the **Hexadecimal** format, your entry **MUST** consist of 64 hexadecimal characters.

The **Cipher Type** is set to **TKIP**.

Define the **GTK update** (Group Transient Key update), or the length of time after which Netkrom AIR-BR500G/GH will automatically generate a new master key.

Press the **Save** button.

Click on **Reboot** to restart the system, after which your settings will become effective.

A **Hexadecimal** value can only take in numbers **0-9** and letters **A-F** and is NOT case-sensitive.

For selecting WPA2-PSK and WPA-PSK-AUTO, you can use the above procedure of selecting WPA-PSK. However, for WPA ( actually is the same as WPA1) , AES is not mandatory whereas AES is mandatory for WAP2.

### 4.5.3 How to set up 802.1x/RADIUS [Available in Access Point mode ONLY]

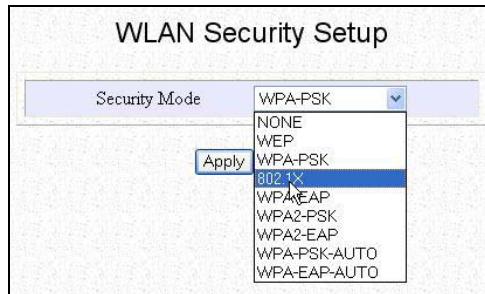
The guidelines below will help you to set up Netkrom AIR-BR500G/GH for using 802.1x/RADIUS.

#### Security Mode –802.1x/RADIUS

At the **WLAN Security Setup** page:

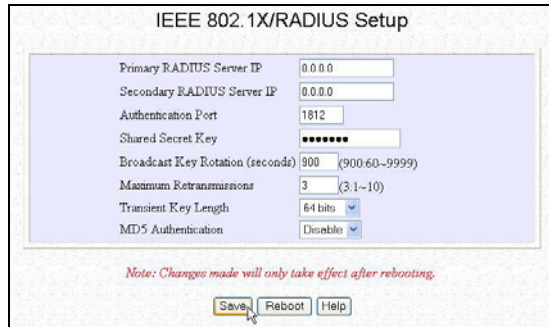
Select **802.1x** mode.

Click on **Apply** button.



Key in the IP address of the **Primary RADIUS Server** in your WLAN.

You can optionally add in the IP address of a **Secondary RADIUS Server**, if any.



[Refer to the section on **How to set up WEP.**]

Press the **Save** button.

Click on **Reboot** to restart the system, after which your settings will become effective.

The RADIUS authentication server **MUST** be in the same subnet as Netkrom AIR-BR500G/GH.

### 4.5.4 How to set up WPA EAP [Available in Access Point mode ONLY]

The guidelines below will help you to set up Netkrom AIR-BR500G/GH for using WPA-EAP. (Please take note that the WPA or WPA1-EAP, WPA2-EAP and WPA-EAP\_AUTO have the same functions).

**Security Mode –WPA-EAP, WPA2-EAP, WPA-EAP-AUTO**

At the **WLAN Security Setup** page:

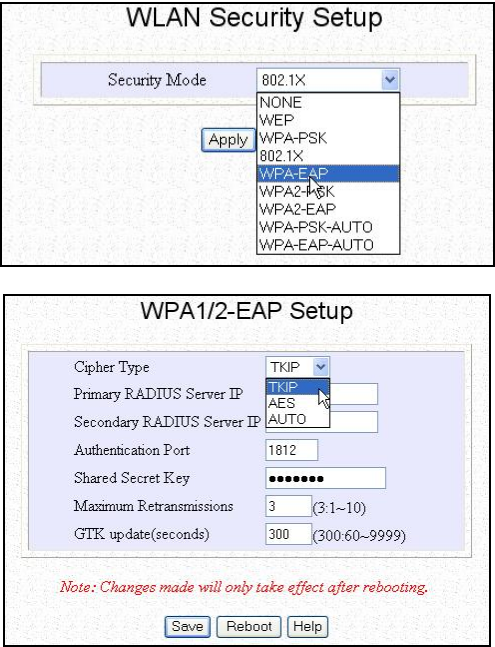
Select **WPA-EAP** mode.

Click on **Apply** button.

The **Cipher Type** is set to TKIP.

Key in the IP address of the **Primary RADIUS Server** in your WLAN.

You can optionally add in the IP address of a **Secondary RADIUS Server**, if any.



The image shows two screenshots of the Netkrom configuration interface. The top screenshot is titled 'WLAN Security Setup' and shows a 'Security Mode' dropdown menu with options: NONE, WEP, WPA-PSK, 802.1X, WPA-EAP (selected), WPA2-PSK, WPA2-EAP, WPA-PSK-AUTO, and WPA-EAP-AUTO. An 'Apply' button is visible. The bottom screenshot is titled 'WPA1/2-EAP Setup' and shows fields for: Cipher Type (TKIP selected), Primary RADIUS Server IP, Secondary RADIUS Server IP, Authentication Port (1812), Shared Secret Key (masked with dots), Maximum Retransmissions (3, range 3-10), and GTK update(seconds) (300, range 300-9999). At the bottom of this page are 'Save', 'Reboot', and 'Help' buttons, and a note: 'Note: Changes made will only take effect after rebooting.'

### Security Mode –WPA-EAP, WPA2-EAP, WPA-EAP-AUTO (continued...)

You can key in a different Authentication Port but it **MUST** match the corresponding port of the RADIUS server.

Enter the **Shared Secret Key**, used to validate client-server RADIUS communications.

Specify the **Maximum Retransmissions**. For greater security, key in the minimum permissible 1, else the maximum allowed is 10.

Define the **GTK update** (Group Transient Key update), or the length of time after which Netkrom AIR-BR500G/GH will automatically generate a new master key.

Press the **Save** button.

Click on **Reboot** to restart the system, after which your settings will become effective.

The RADIUS authentication server **MUST** be in the same subnet as Netkrom AIR-BR500G/GH.

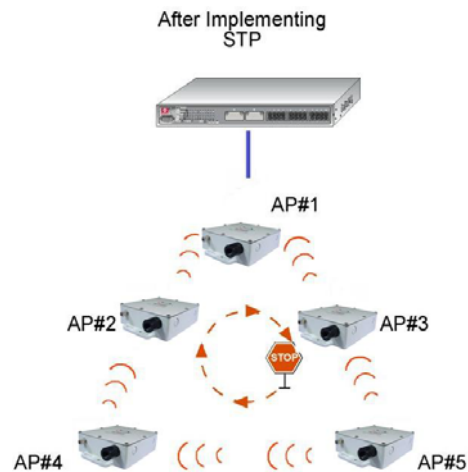
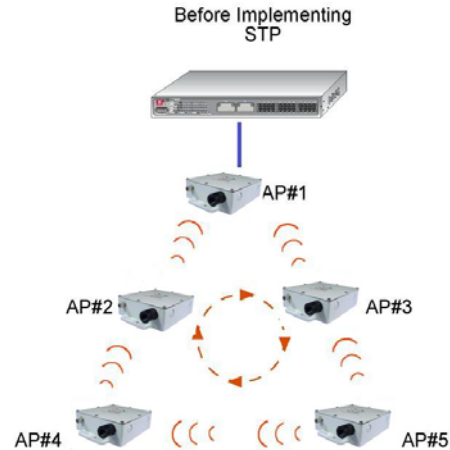
For selecting WPA2-EAP and WPA-EAP-AUTO, you can use the above procedure of selecting WPA-EAP. However, for WPA ( actually is the same as WPA1) , AES is not mandatory whereas AES is mandatory for WPA2.

### 4.6 STP Setup ( available in AP/Gateway modes)

Spanning Tree Protocol (STP) is a link management [protocol](#) that helps to prevent undesirable loops occur in the network. For an Ethernet network to function properly, only one active path can exist between two stations. If a loop exists in the network topology, duplication of messages will occur and this might confuse the forwarding algorithm and allow duplicate frames to be forwarded.

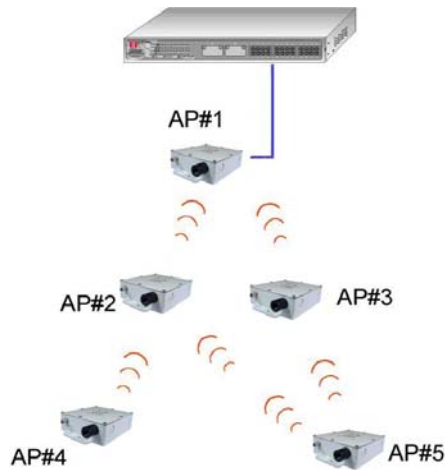
In short, the main purpose of activating STP is to prevent looping when you have redundant paths in the network. Without activating STP, redundant topology will cause broadcast storming.

To establish path redundancy, STP creates a [tree](#) that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree [topology](#) and re-establishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the [LAN](#).



Spanning-Tree Protocol operation is transparent to end stations, which are unaware whether they are connected to a single LAN segment or a switched LAN of multiple segments.

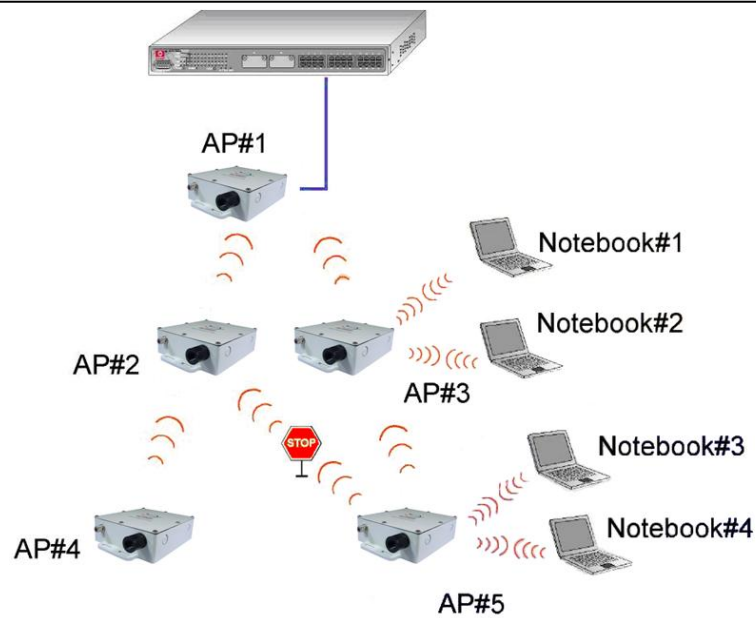
The figure shown below explains the implementation of STP in a network. AP#1 is physically connected to a switch whilst another 4 access points (AP#2, AP#3, AP#4 and AP#5) are connected to AP#1 wirelessly. Redundant paths were found in this network, without enabling STP function, broadcast storm will occur in this network, resulted duplicated frames to be forwarded.



When STP is enabled, the STP-enabled access points will first try to find the root access point using the following criteria:

- a. use the access point that is configured with the smallest STP priority. Default priority set in the access points is 32768.
- b. If the STP priority values are the same, the access point with smallest MAC address will be chosen as root.





Once the root access point is determined, the STP algorithm will start to calculate the path cost from each access point to the root access point. Based on the path cost in the following table,

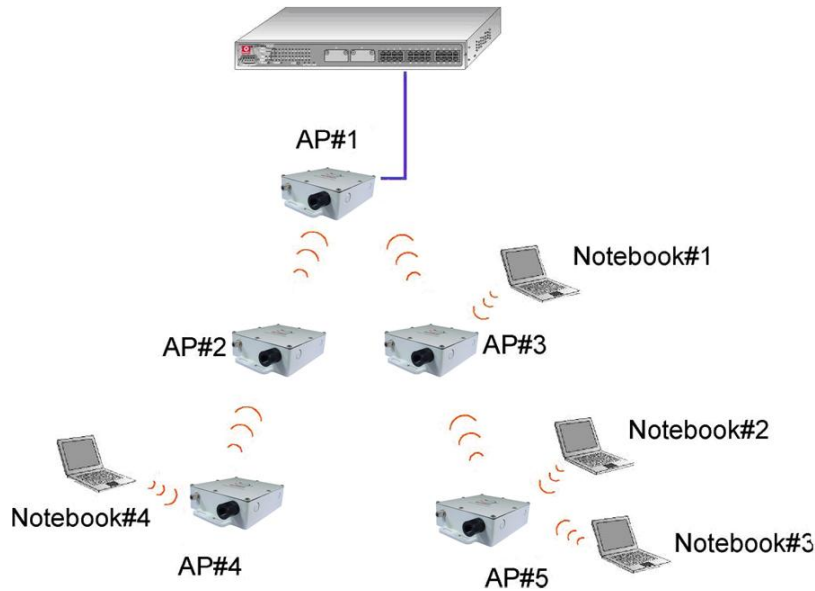
Bandwidth	STP Cost
4Mbps	250
10Mbps	100
16Mbps	62
45Mbps	39
100Mbps	19
155Mbps	14
622Mbps	6
1Gbps	4
10Gbps	2

The path with the smallest cost will be used and extra redundant paths will be disabled.

To explain the effect of STP & Pseudo VLAN on the wireless clients, we will compare 3 separate scenarios.

### **Scenario #1 – (No STP, No Pseudo VLAN)**

Referring to the illustration below, if the Spanning Tree Protocol (STP) and Pseudo VLAN are not implemented in a network, all clients (Notebook#1, #2, #3 & #4,) can access to one another, resulting low level of data security. If redundant paths were found in this network, broadcast packets will be duplicated and forwarded endlessly resulting in a broadcast storm.

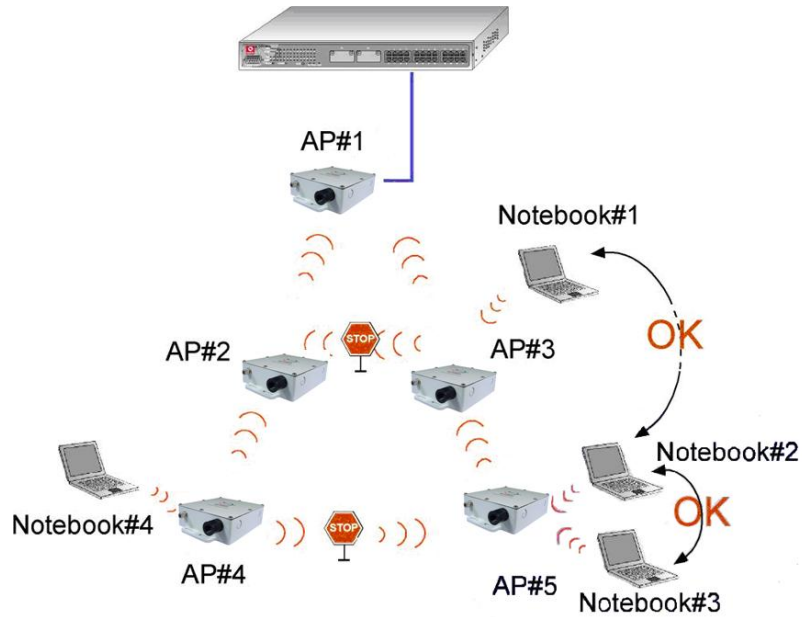


### **Scenario #2 – (With STP, No Pseudo VLAN)**

When STP is enabled, extra redundant network paths between access points will be disabled, hence preventing multiple active network paths in between any two network access points.

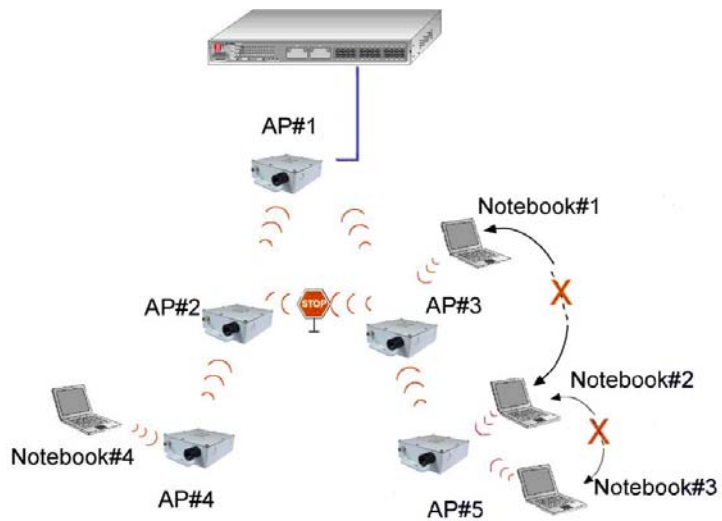
If one of the access points is down, the STP algorithm will reactivate one of the redundant paths so that the network connection will not be lost.

All wireless users will be able to communicate with each other if they are associated to the access points of the same WDS zone.



**Scenario #3 – (With STP and Pseudo VLAN)**

In this example, both STP and Pseudo VLAN are implemented in this network. All wireless users are unable to communicate with one another. This is one of the measures to ensure data privacy between wireless users in the network.



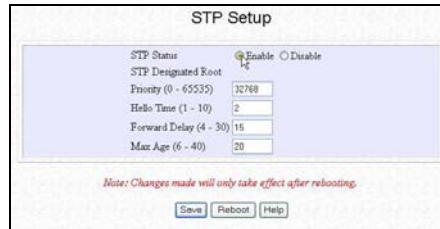
### Enabling STP Setup

Click on **STP Setup** from the **CONFIGURATION** menu

Select **Enable** from the **STP Status** radio button.

#### STP Status:

Activate Spanning Tree Protocol (STP) function makes your network more resilient to link failure and also provides a protection from loop.



#### Priority:

Specify the configurable value that is appended as the most significant portion of a AP.

This value specifies which access point acts as the central reference point, or Root AP, for the STP system — the lower the priority value, the more likely the access point is to become the Root AP. If the priority values are all the same, then the system will search for the smallest MAC address of the access point and set it as the Root AP.

#### Hello Time:

Specify the time in seconds that elapses between the configuration messages (also known as Hello BPDUs) generated by an AP that assumes itself to be the Root AP.

#### Forwarding Delay:

Specify the time in seconds that an AP spends in the listening and learning states, that is, listening for configuration messages.

#### Max Aging Time:

Specify the maximum age in seconds at which the stored configuration message information is judged to be too old and is discarded.

If an AP does not receive a configuration message after the Max Aging Time, the system will assume that the link between itself and the Root AP has gone down and will then reconfigures the network to cater for the change.

Click on the **Apply** button.

### 4.7 SNMP Setup

Simple Network Management Protocol (SNMP) is a set of communication protocols that separates the management architecture from the architecture of the hardware devices.

**Enabling SNMP**

Click on **SNMP Setup** from the **CONFIGURATION** menu

SNMP Setup

SNMP State

Enable

Read Password

\*\*\*\*\*

Read/Write Password

\*\*\*\*\*

Apply

Select **Enable** from the **SNMP State** drop-down list.

The default **Read Password** is set to *public* while the default **Read/Write Password** is *private*.

Click on the **Apply** button.

### 4.8 MAC Filtering

MAC Filtering acts as a security measures by controlling the users from accessing to the network. This can be easily done by adding the user's MAC address to the listing and from there, you can choose whether the particular user is allowed to access to the network or not. Simply click on the radio button besides **Allow PCs listed to access network**, or **Prevent PCs listed from accessing network** to activate the function.

### Enabling MAC Filtering

Click on **MAC Filtering** from the **CONFIGURATION** menu.

Select **Enable** from the **MAC Filtering** drop-down list.

Click on the **Add** button to add in the MAC address of the user.

Fill in the **Filtered Mac Address** field with the MAC address of the client in the format **xx:xx:xx:xx:xx:xx** or **xx-xx-xx-xx-xx-xx**, where x is any value within the range 0-9 or a-f.

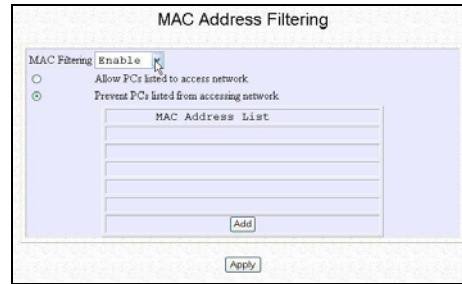
Click on the **Apply** button to update the changes.

Referring to the figure shown on the right, notice that the MAC Address has been added to the list.


Next, you can choose whether you wish to allow/prevent the user to/from access to the network.

Simply click on the radio button besides Allow PCs listed to access network, or Prevent PCs listed from accessing network.

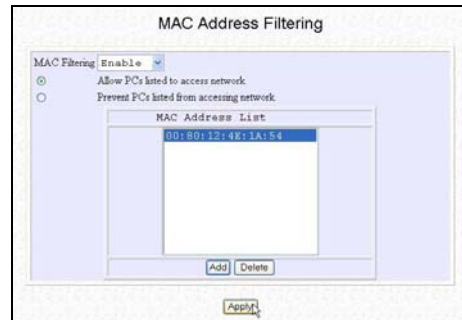
Click **Apply** button to update the changes.



The screenshot shows the 'MAC Address Filtering' window. At the top, 'MAC Filtering' is set to 'Enable'. Below this, there are two radio buttons: 'Allow PCs listed to access network' (which is selected) and 'Prevent PCs listed from accessing network'. Underneath, there is a table titled 'MAC Address List' with several empty rows. At the bottom right of the table is an 'Add' button, and at the very bottom of the window is an 'Apply' button.



The screenshot shows the 'Add MAC Address' dialog box. It contains a single text field labeled 'Filtered MAC Address' with the value '00-80-12-4e-1a-54' entered. Below the text field is an 'Apply' button.



The screenshot shows the 'MAC Address Filtering' window again. The 'MAC Filtering' dropdown is still 'Enable'. The 'Allow PCs listed to access network' radio button is still selected. The 'MAC Address List' table now contains one entry: '00:80:12:4E:1A:54'. At the bottom right of the table are 'Add' and 'Delete' buttons, and at the very bottom of the window is an 'Apply' button.



#### NOTE

When Mac Filtering is enabled with allow access policy, the Mac Address list cannot be empty.

### Chapter 5 Further Configuration

This chapter provides guidelines in:

- **Setting up uConfig (only in Gateway mode)**
- **Configuring WAN Setup (only in Gateway or Wireless Routing Client mode)**
- **Using NAT**
- **Routing**
- **Implementing IP Filtering**
- **Applying Remote Management**
- **Enabling Parallel Broadband**

#### 5.1 Setting up uConfig (only in Gateway mode)

This option is ONLY available when Netkrom AIR-BR500G/GH operates in **Gateway** mode.

**uConfig Set up**

Click on **uConfig IP Setup** from the **CONFIGURATION** menu.

Fill in the IP Address.

Key in the **Network Mask**.

Click on **Save** button.

**Reboot** the system to make your changes effective.

uConfig IP Setup

IP Address	192	160	254	254
Network Mask	255	255	255	0

*Note: Changes made will only take effect after rebooting.*

Save

Reboot

### 5.2 Configuring WAN Setup (Available in Gateway and Wireless Routing Client mode)

The WAN setup allows you to set up Netkrom AIR-BR500G/GH for broadband Internet connection.

Described below are the common steps you should start with to select or change the broadband connection type.

#### Changing WAN Type

Click on **WAN Setup** from the **CONFIGURATION** menu.

The setup page of the WAN type that you have last implemented will be displayed.

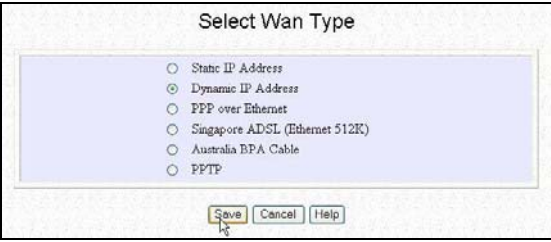
Since Netkrom AIR-BR500G/GH operates in **Dynamic IP** Address Allocation mode by default, initially the **Dynamic IP** setup page will appear.

Press the **Change** button (which appears on the setup pages of all the WAN Types), to reach the **Select WAN Type** page.

Select the **WAN type** you want to switch to.

Click on **Save**.

The setup page of the WAN type that you have selected will then appear.





### 5.2.1 Dynamic IP

In the default **dynamic IP** addressing mode, your ISP automatically assigns the IP address of Netkrom AIR-BR500G/GH to it.

This type of connection applies to most Cable Internet subscribers, for instance:

- Cable Vision subscribers.
- @HOME Cable Service users.

#### Changing WAN Type – Dynamic IP Configuration

At the **Dynamic IP WAN Setup** page:

You can review the:

- IP Address
- Network Mask
- Gateway IP Address
- Primary DNS
- Secondary DNS

The screenshot shows the 'WAN Setup' window with a 'Dynamic IP' tab selected. A 'Change' button is visible in the top right corner of the configuration area. The configuration table is as follows:

Wan Type	Dynamic IP
IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Your ISP dynamically allocates these parameters to Netkrom AIR-BR500G/GH.

### 5.2.2 Static IP

If you have subscribed to a specific IP address or to a fixed range of IP addresses from your ISP, follow the procedure summarized below.

#### Changing WAN Type – Static IP Configuration

At the **Static IP WAN Setup** page:

Replace the default **IP Address**, **Network Mask** and **Gateway IP Address** fields with the relevant values given by your ISP.

The screenshot shows the 'WAN Setup' window with a 'Static IP' tab selected. The configuration table is as follows:

Wan Type	Static IP
IP Address	203.120.12.240
Network Mask	255.255.255.0
Gateway IP Address	203.120.12.2

Below the table, there is a note: "Note: Changes made will only take effect after rebooting." At the bottom, there are three buttons: 'Save', 'Reboot', and 'Help'. A mouse cursor is pointing at the 'Save' button.

Click on the **Save** button.

Click on the **Reboot** button to restart the system and let the changes to take effect.

### 5.2.3 PPPoE

Select this connection type if you have subscribed to ADSL in a country utilizing standard PPPoE for authentication, for instance:

- If you are in Germany which uses T-1 connection.
- If you are a SingNet Broadband or Pacific Internet Broadband user in Singapore.

The next steps will guide you in setting up Netkrom AIR-BR500G/GH.

#### Changing WAN Type – PPPoE Configuration

At the **PPPoE WAN Setup** page:

Fill in the relevant fields following the parameters of your broadband Internet account.

The **Status** section gives you a summary of your connection settings such as:

- IP address
- Network Mask
- Gateway IP Address
- Primary & Secondary DNS

The screenshot shows the 'WAN Setup' configuration page. At the top, 'Wan Type' is set to 'PPPoE' with a 'Change' button next to it. Below this, 'MTU(1400 - 1492)' is set to '1462' (default 1462). There are input fields for 'Username' and 'Password' (masked with asterisks), and a 'Service Name' field. Connection options include 'On-Demand' (selected), 'Always-On', and 'Use non-standard PPPoE ethernet type' (unchecked). 'Idle Timeout (0/Disable)' is set to '0' seconds, and 'Reconnect Time Factor' is set to '30' seconds. The 'Status' section shows 'Disconnected' with a 'Connect' button. Below the status, IP settings are listed: 'IP Address' (0.0.0.0), 'Network Mask' (0.0.0.0), 'Gateway IP Address' (0.0.0.0), 'Primary DNS' (0.0.0.0), and 'Secondary DNS' (0.0.0.0). At the bottom, there are 'Save', 'Reboot', and 'Help' buttons. A note at the bottom states: 'Note: Changes made will only take effect after rebooting.'

If you are offline, pressing the **Connect** button will immediately initiate a connection.

Click on the **Save** button.

Click on the **Reboot** button to restart the system and allow the changes to take effect.

PPPoE Parameter	Description
<b>MTU</b>	The MTU or Maximum Transmission Unit is the largest packet size allowed by the ISP. It is set by default to <b>1462</b> though it can vary between 1400 and 1492.
<b>Username</b>	This refers to your broadband account username.
<b>Password</b>	This refers to your broadband account password.
<b>Service Name</b>	This optional field allows you to key in the service name of your ADSL subscription.
<b>On-Demand</b>	If enabled, the Netkrom AIR-BR500G/GH router will automatically connect to the ISP whenever a LAN client makes an Internet request.
<b>Idle Timeout</b>	<p>This field is relevant only if the <b>On-Demand</b> option is enabled and allows you to specify a maximum lapse of idle time allowed before Netkrom AIR-BR500G/GH automatically goes offline. It will only re-connect when a LAN client makes an Internet request.</p> <p>If the field is set to <b>0</b>, this feature will be disabled and Netkrom AIR-BR500G/GH will remain online unless disconnected by the ISP.</p>
<b>Always-On</b>	If this feature is enabled, Netkrom AIR-BR500G/GH will remain permanently connected to the Internet.
<b>Reconnect Time Factor</b>	This field is relevant only if the <b>Always-On</b> option is enabled and allows you to specify a maximum lapse of offline time following which, Netkrom AIR-BR500G/GH should automatically reconnect to the Internet. The default value has been set to <b>30</b> seconds.
<b>Use non-standard PPPoE Ethernet type</b>	This applies to certain Ethernet-based ADSL modem requiring non-standard PPPoE for authentication. In case of doubts, do <u>NOT</u> enable this checkbox.

### 5.2.4 Singapore ADSL

Other ADSL subscribers in Singapore, including SingTel Magix SuperSurf users, should opt for this type of connection.

#### Changing WAN Type – Singapore ADSL Configuration

At the **Singapore ADSL WAN Setup** page:

Key in the **Username** of your Internet account.

Insert your account **Password**.

Enter an **Idling Timeout** value, in the range of 30-3600 seconds. Entering **0** will disable this feature.

The screenshot shows the 'WAN Setup' window. It has a title bar 'WAN Setup'. Inside, there's a table-like structure with labels on the left and values on the right. The labels are: Wan Type, Username, Password, Idle Timeout (30-3600, 0:Disable), Status, IP Address, Network Mask, Gateway IP Address, Primary DNS, and Secondary DNS. The values are: Singapore ADSL(Ethernet 512K), Username@INT512, a masked password (\*\*\*\*\*), 300 seconds, Disconnected, 0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0, and 0.0.0.0. There are 'Change' and 'Connect' buttons. Below the table, there's a red note: 'Note: Changes made will only take effect after rebooting.' At the bottom, there are 'Save', 'Reboot', and 'Help' buttons.

Wan Type	Singapore ADSL(Ethernet 512K)	<a href="#">Change</a>
Username	Username@INT512	
Password	*****	
Idle Timeout (30-3600, 0:Disable)	300	seconds
Status	Disconnected	<a href="#">Connect</a>
IP Address	0.0.0.0	
Network Mask	0.0.0.0	
Gateway IP Address	0.0.0.0	
Primary DNS	0.0.0.0	
Secondary DNS	0.0.0.0	

*Note: Changes made will only take effect after rebooting.*

[Save](#) [Reboot](#) [Help](#)

The **Status** section gives you a summary of your connection settings such as:

- IP address
- Network Mask
- Gateway IP Address
- Primary & Secondary DNS

If you are offline, pressing the **Connect** button will immediately initiate a connection.

Click on the **Save** button.

Press the **Reboot** button to restart the system and allow the changes to take effect.

### 5.2.5 Australia BPA Cable

This type of connection has been especially customized for Big Pond Cable Internet users in Australia

#### Changing WAN Type – Singapore ADSL Configuration

At the **Australia BPA WAN Setup** page:

Key in the **Username** of your Internet account.

Insert your account **Password**.

Enter the **IP address** of your Authentication Server, as defined by your ISP.

Fill in an **Idling Timeout** value, in the range of 30-3600 seconds.

Entering **0** will disable this feature.

The Status section gives you a summary of your connection settings such as:

- IP address
- Network Mask
- Gateway IP Address
- Primary & Secondary DNS

If you are online, pressing the **Disconnect** button will immediately end your connection.

Click on the **Save** button.

Press the **Reboot** button to restart the system and allow the changes to take effect.

The screenshot shows the 'WAN Setup' window with the following fields and values:

WAN Setup	
Wan Type	Australia BPA Cable <span>Change</span>
Username	<input type="text" value="Username"/>
Password	<input type="password" value="*****"/>
Authentication Server	<input type="text"/>
Idle Timeout (30-3600, 0 Disable)	<input type="text" value="0"/> seconds
Status	Disconnected <span>Connect</span>
IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

*Note: Changes made will only take effect after rebooting.*

Save Reboot Help

### 5.2.6 PPTP

The Point-to-Point Tunnelling Protocol (PPTP) is a networking technology which, enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks, enabling remote users to access corporate networks securely at a lower cost

#### Changing WAN Type – PPTP Configuration

At the **PPTP WAN Setup** page:

Key in the **Client IP address**.

Enter the **Network Mask**.

Fill in the **Username** of your Internet account.

Insert your account **Password**.

Enter the **IP address** of your VPN Server.

Fill in an **Idling Timeout** value, in the range of 30-3600 seconds.

Entering **0** will disable this feature.

Click on the **Save** button.

Press the **Reboot** button to restart the system and let the changes take effect.

The screenshot shows the 'WAN Setup' window with the following fields and values:

Field	Value
Wan Type	PPTP
Client IP	203.120.12.240
Net Mask	255.255.255.0
Username	Username
Password	*****
VPN Server	
Idle Timeout (30-3600, 0 Disable)	0 seconds
Status	Disconnected
IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Buttons: Change, Connect, Save, Reboot, Help.

Note: Changes made will only take effect after rebooting.

### 5.3 Using NAT (Only available in Gateway and Wireless Routing Client mode)

NAT, also known as Network Address Translation, functions by transforming the private IP address of packets originating from hosts on your network so that they appear to be coming from a single public IP address and by restoring the destination public IP address to the appropriate private IP address for packets entering the private network. The multiple PCs on your network would then appear as a single client to the WAN interface.

**Enabling NAT**

Click on **NAT** from the **CONFIGURATION** menu.

By default, the **NAT Status** radio button is enabled.

To change the **NAT Status**:

Select the appropriate radio button.

Click on the **Apply** button.

**Enable/Disable NAT**

NAT Status

☒ Enable ☐ Disable

Apply

Help

**Advanced NAT Options**

DMZ

Port Forwarding



#### NOTE

Disabling NAT will disable Internet Sharing. Broadband Internet sharing requires this option to be Enabled.

When NAT is enabled, your network is not accessible to the WAN. However, implementing **virtual servers** allows you to host Internet servers such as Web servers, FTP servers or Mail servers on your network, in spite of NAT.

### 5.3.1 To set up a De-Militarised Zone host

A De-Militarised Zone host, or DMZ host, is a separate neutral client sitting between your private network and the WAN.

It initiates WAN connections upon request from your network clients, and forwards the request packets. Similarly, outside users can access only the DMZ host.

You can host Web pages or public information that can be served to the outside world, on the DMZ host.

**Setting up DMZ**

Click on **NAT** from the **CONFIGURATION** menu.

Ensure the **NAT Status** is enabled.

At the **Advanced NAT Options** section:

Click on **DMZ**.

Key in the **IP address** of the PC you wish to place within the DMZ in the **Private IP Address** field.

The default Private IP Address is set to 0.0.0.0. For illustration, we entered **192.168.168.55**

Click on the **Apply** button to confirm your entry.

**Nat DMZ Ip Address**

Private IP Address: 192.168.168.55

Apply

**Disable DMZ**

Enter **0.0.0.0** as the **Private IP Address**.

Click on the **Apply** button.

**Nat DMZ Ip Address**

Private IP Address: 0.0.0.0

Apply

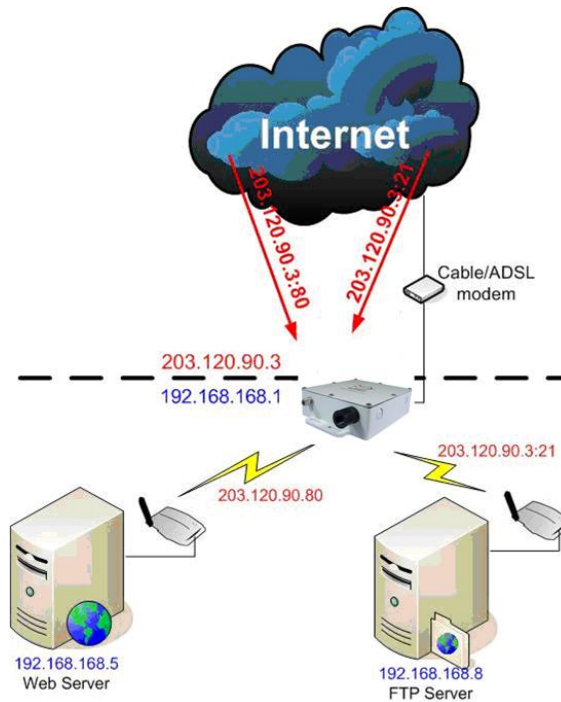


### 5.3.2 To set up port forwarding

Port forwarding allows Netkrom AIR-BR500G/GH to redirect any incoming Internet request bearing a public IP address to a specific PC on your network, based on the incoming packet's TCP/UDP port number.

You can thus use TCP port forwarding to hide your web-server behind Netkrom AIR-BR500G/GH for added security while using UDP port forwarding lets you run a secure multiplayer game server.

The following diagram shows a Netkrom AIR-BR500G/GH with a public IP address of 203.120.90.3 and a private IP address of 192.168.168.1. All incoming packets with port number 80 will be forwarded to the Web server, known on the LAN as 192.168.168.5, while those with port number 21 will be directed to the FTP server which has a private IP address of 192.168.168.8.

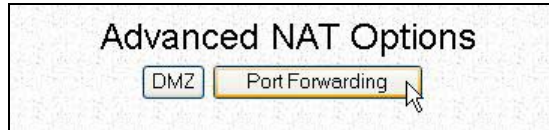


### Set up Port Forwarding – For Known Server

Click on **NAT** from the **CONFIGURATION** menu.

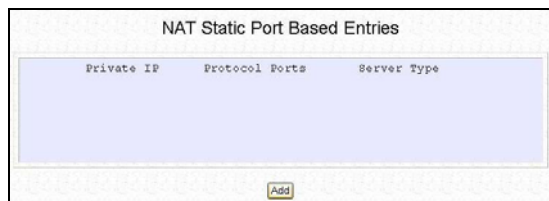
Ensure whether the **NAT Status** is enabled.

At the **Advanced NAT Options** section:



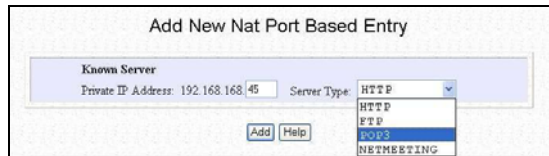
Click on **Port Forwarding**.

The **NAT Static Port Based Entries** table illustrated by the screen shot displays the list of current port-based entries.



Click on the **Add** button.

For standard server applications: **HTTP/FTP/POP3/Netmeeting**, go to the **Known Server** section:



Complete the **Private IP Address** field.

Pick the appropriate selection from the **Server Type** drop down list.

Click on **Add** button.

We illustrated with a **POP3** server having **Private IP Address** of **192.168.168.45**.

### Set up Port Forwarding – For Custom Server

Otherwise, in order to set up Internet applications which are not defined in the **Known Server** section, go to **Custom Server**:



The screenshot shows a 'Custom Server' configuration window. It contains the following fields: 'Private IP Address' with the value '192.168.168.55', 'Protocol' with a dropdown menu showing 'UDP', 'Ports' with a range '15-89', and 'Server Type' with a dropdown menu showing 'LAN Game'. There is an 'Add' button at the bottom right.

Key in the **Private IP Address**.

Define the **Port numbers** to use.

Select the relevant **Protocol** from the drop down list.

Identify the **Server Type**.

Click on **Add** button.

We entered a **Private IP Address** of **192.168.168.55**, defined ports **15** to **89** as the application **Ports**, selected **UDP** from the **Protocol** drop-down list and labelled the **Server Type** as **LAN Game**.

The updated **NAT Static Port Based Entries** will reflect your new entry.

If you want to assign more servers in your LAN, click on the **Add** button.

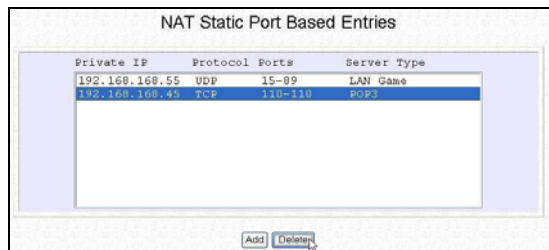
### Delete a table entry

If you want to delete any of the table entries:

Select the entry to delete.

Click on the **Delete** button.

The table will be refreshed.



The screenshot shows a table titled 'NAT Static Port Based Entries'. The table has four columns: 'Private IP', 'Protocol', 'Ports', and 'Server Type'. There are two entries in the table. The second entry is selected (highlighted in blue).

Private IP	Protocol	Ports	Server Type
192.168.168.55	UDP	15-89	LAN Game
192.168.168.45	TCP	110-110	POP3

At the bottom of the window, there are 'Add' and 'Delete' buttons.

The following is a non-exhaustive list of well-known port numbers:

Application	Port Number
Echo	7
Daytime	13
FTP	21
SMTP (Simple Mail Transfer, i.e., email)	25
Telnet	23
Time	37
Name server	42
Gopher	70
WWW (World Wide Web)	80

### 5.4 Routing (Only available in Gateway and Wireless Routing Client mode)

Netkrom AIR-BR500G/GH supports both static routing so that you can manually add entries into its routing table and dynamic routing, where it will automatically update the routing table, whenever necessary.



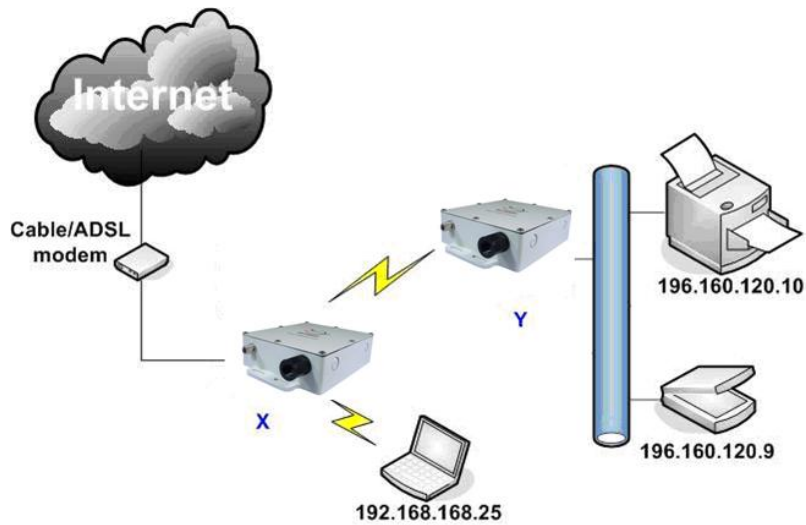
#### NOTE

The default settings of Netkrom AIR-BR500G/GH are sufficient to allow broadband Internet sharing. There is NO need to configure any further routing information.

**Please note that improper routing settings will cause undesired effects!**

The diagram illustrates a Netkrom AIR-BR500G/GH (**X**) functioning as Internet gateway to wireless clients while another Netkrom AIR-BR500G/GH (**Y**) connects to the office's remote resources.

The routing table of **X** can be modified so that if its wireless clients intend to use the remote office resources, data packets are automatically redirected to **Y**.



### 5.4.1      Static Routing

The following will show you how to add entries to your gateway's routing table so that it may re-route IP packets to another network, which is very useful if your network has more than one router.

### Static Routing

Click on **Routing** from the **CONFIGURATION** menu.

The **IP Routing Table** illustrated by the screen shot on the left displays the list of current routing entries.

If you want to add a static route in the **IP Routing Table**:

Click on the **Add** button.

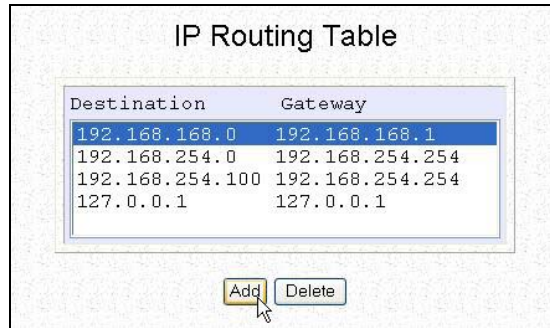
Specify the **Destination IP Address** of your new entry.

Fill in the **Gateway IP Address**.

Click on **Apply**.

The new entry will appear in the updated **IP Routing Table**.

If you want to add more routes, click on the **Add** button.



The screenshot shows a window titled "IP Routing Table". Inside, there is a table with two columns: "Destination" and "Gateway". The table contains four entries. The first entry, "192.168.168.0" for "192.168.168.1", is highlighted with a blue background. Below the table are two buttons: "Add" and "Delete". A mouse cursor is pointing at the "Add" button.

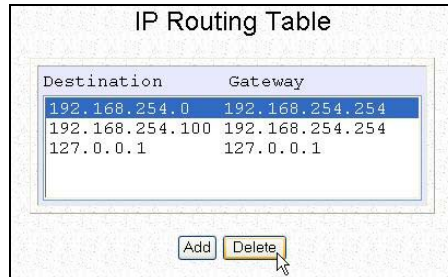
Destination	Gateway
192.168.168.0	192.168.168.1
192.168.254.0	192.168.254.254
192.168.254.100	192.168.254.254
127.0.0.1	127.0.0.1

### Delete Static Routing

If you want to delete any of the table routes:

Select the entry to delete. Click on the **Delete** button.

The table will be refreshed.



The screenshot shows the "IP Routing Table" window after a deletion. The table now has three entries. The first entry, "192.168.254.0" for "192.168.254.254", is highlighted with a blue background. The "Add" and "Delete" buttons are still present at the bottom, with a mouse cursor pointing at the "Delete" button.

Destination	Gateway
192.168.254.0	192.168.254.254
192.168.254.100	192.168.254.254
127.0.0.1	127.0.0.1

### 5.4.2 Dynamic Routing

When using dynamic routing, Netkrom AIR-BR500G/GH can continuously update its routing table with the latest routing information, thus automatically adjusting to any physical changes in the network topology.

Netkrom AIR-BR500G/GH supports RIP1 (Routing Information Protocol) and RIP2 (Routing Information Protocol version 2), and periodically broadcasts its routing tables to neighboring routers. The best route is chosen if there are multiple routes to a destination.

The next steps will guide you in setting up dynamic routing.

### Dynamic Routing

Click on **Routing** from the **CONFIGURATION** menu.

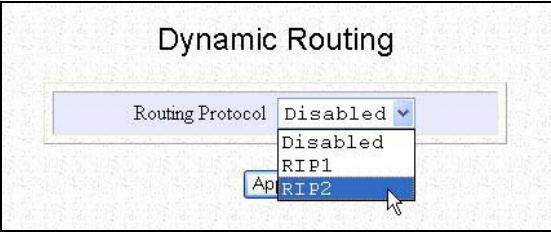
By default, **Dynamic Routing** is disabled.

Select which dynamic routing protocol to implement from the **Routing Protocol** drop down list.

Click on the **Apply** button.

**Reboot** the system.

From then on, the **IP Routing Table** will be dynamically updated.



### 5.5 Implementing IP Filtering (Only available in Gateway and Wireless Routing Client mode)



Enabling the IP Filtering function causes Netkrom AIR-BR500G/GH to decide, according to predefined rules, whether to block all outgoing packets or to let them pass.

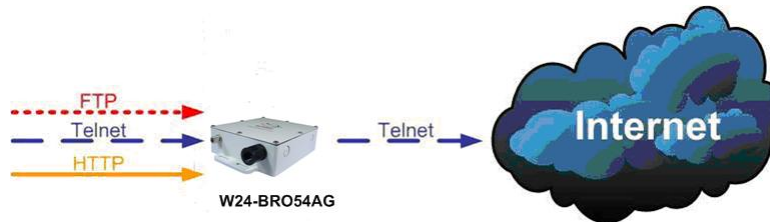
Netkrom AIR-BR500G/GH provides granularity and latitude in monitoring the traffic in your network by allowing you to define IP filtering rules, based on these 3 factors:

- **Source IP Address**  
This would allow you to selectively restrict Internet activity originating from a specific PC or group of PCs.
- **TCP Port**  
You may choose to prevent certain applications such as FTP or Telnet, which use a commonly known port number.
- **Time frame**  
For example, you may restrict Internet access from your children's PC to certain time frames such as between 19H30 and 21H45.

For instance, let us assume that an IP filtering rule has been defined as:

TCP Port **23** from **any** IP on **any** day at **any** time (Port 23 is usually used for **Telnet**).

If the **sent** radio button is selected, all outgoing packets will be sent except those belonging to **Telnet** sessions. On the other hand, if the **discarded** radio button is selected, all outgoing packets will be blocked except for those belonging to **Telnet** sessions. We illustrated the second case below.



### IP Filtering

Click on **IP Filtering** from the **CONFIGURATION** menu.

Select either the **Sent** or **Discarded** radio button to accept or reject any packet conforming to the rules.

Click on the **Add** button to set the new rule in the **IP Filter Configuration** GUI.

The screenshot shows the 'Filtering Configuration' window. At the top, a warning states: 'Warning: Incorrect configuration may cause undesirable behavior.' Below this, a text line says: 'All IP packets will be ☒ sent ☐ discarded except for those matching one or more of the following rules.' There is a table with columns: 'Select to Edit', 'Rule Name', 'IP Address(es)', 'Destination Port(s)', 'Day of the Week', and 'Time of the Day'. The first row has a radio button under 'Select to Edit' and is empty for the other fields. Below the table, a text line says: 'If the system loses its time settings, ☒ ignore ☐ accept the access time settings in the above rules.' At the bottom are buttons: 'Apply', 'Add', 'Delete', 'Edit', and 'Help'. A mouse cursor is pointing at the 'Add' button.

Insert a **Rule Name** for this new packet filtering rule.

A text input field labeled 'Rule Name' containing the text 'Office'.

From the **IP Address** drop down list, select whether to apply the rule to:

A dropdown menu for 'IP Address' with options: 'Range', 'Any', 'Single'. The 'Range' option is selected. Below the dropdown are two input fields: '(From)' with '192.168.168.25' and '(To)' with '192.168.168.75'.

### A Range of IP addresses

In this case, you will have to define **(From)** which IP address **(To)** which IP address, your range extends.

The 'IP Address' dropdown is set to 'Range'. The '(From)' field contains '192.168.168.25' and the '(To)' field contains '192.168.168.75'.

### A Single IP address

Here, you need only specify the source IP address in the **(From)** field.

The 'IP Address' dropdown is set to 'Single'. The '(From)' field contains '192.168.168.25' and the '(To)' field is empty.

### Any IP address

You may here, leave both, the **(From)** as well as the **(To)** fields, blank.

The 'IP Address' dropdown is set to 'Any'. Both the '(From)' and '(To)' fields are empty.

### IP Filtering (continued...)

At the **Destination Port** drop

down list, select either:

### A Range of TCP ports

In this case, you will have to define **(From)** which port **(To)** which port, your rule applies.

### A Single TCP port

Here, you need only specify the source port in the **(From)** field.

### Any IP port

You may here, leave both, the **(From)** as well as the **(To)** fields, blank.

From the **Day of the Week** drop down list, select whether the rule should apply to:

### A Range of days

Here, you will have to select **(From)** which day **(To)** which day

### Any day

In this case, you may skip both the **(From)** as well as the **(To)** drop down fields.

Destination Port	Single
(From)	Any
(To)	Range

Destination Port	Range
(From)	25
(To)	61

Destination Port	Single
(From)	25
(To)	

Destination Port	Any
(From)	
(To)	

Day of the Week	Range
(From)	Any
(To)	Range

Day of the Week	Range
(From)	Mon
(To)	Thu

Day of the Week	Any
(From)	Sun
(To)	Sun

IP Filtering (continued...)

## Chapter 5 Further Configuration

At the **Time of the Day** drop down list, you may also choose to apply the rule to:

### A Range of time

In which case, you have to specify the time in the format **HH:MM**, where **HH** may take any value from 00 to 23 and **MM**, any value from 00 to 59.

### Any time

Here, you may leave both **(From)** and **(To)** fields blank.

Time of the Day	Range	(hh: 00-23, mm: 00-59)
(From)	Any	(hh:mm)
(To)	15:00	(hh:mm)

Time of the Day	Range	(hh: 00-23, mm: 00-59)
(From)	08:00	(hh:mm)
(To)	15:00	(hh:mm)

Time of the Day	Any	(hh: 00-23, mm: 00-59)
(From)		(hh:mm)
(To)		(hh:mm)

Click on the **Apply** button to make the new rule effective.

The **Filtering Configuration** table will then be updated.

If you want to define more **IP Filtering** rules, click on the **Add** button.

### Delete IP Filtering

We illustrated deleting the rule called **Finance**.

To delete an existing IP filtering rule:

Select the radio button corresponding to the rule to delete.

Click on **Delete**.

The **Filtering Configuration** table will then be refreshed.

**Filtering Configuration**

*Warning: incorrect configuration may cause undesirable behavior.*

All IP packets will be ☒ sent ☐ discarded except for those matching one or more of the following rules.

Selected to Edit	Rule Name	IP Address(es)	Destination Port(s)	Day of the Week	Time of the Day
<input checked="" type="radio"/>	Finance	192.168.168.12-192.168.168.16	1-5	Mon-Fri	08:00-15:00
<input type="radio"/>	Purchasing	192.168.168.20-192.168.168.30	14-24	Mon-Sat	09:00-22:00

If the system loses its time settings, ☒ ignore ☐ accept the access time settings in the above rules.

[Apply](#) [Add](#) [Delete](#) [Edit](#) [Help](#)

### Delete IP Filtering (continued...)

We illustrated editing the rule called **Purchasing**.

If you want to edit an existing IP filtering rule:

Select the radio button corresponding to the rule to edit.

Click on **Edit**.

You will then return to the **IP Filtering Configuration** GUI, from which you can re-define the rule.

**Filtering Configuration**

*Warning: Incorrect configuration may cause undesirable behavior.*

All IP packets will be ☒ sent ☐ discarded except for those matching one or more of the following rules.

Select to Edit	Rule Name	IP Address(es)	Destination Port(s)	Day of the Week	Time of the Day
<input checked="" type="radio"/>	Purchasing	192.168.168.20-192.168.168.30	14-24	Mon-Sat	09:00-22:00

If the system loses its time settings, ☒ ignore ☐ accept the access time settings in the above rules.

### 5.6 Applying Remote Management (Only available in Gateway and Wireless Routing Client mode)

Making use of remote management, you only require Internet access to be able to manage your network.

This feature is especially helpful for those who work away from the office or from home.

#### Remote Management

Click on **Remote Management** from the **CONFIGURATION** menu.

Specify the **HTTP Port number** and the **Telnet Port number**.

The standard entry for HTTP Port is 80 and 23 for Telnet Port.

Click on **Save** button.

Press the **Reboot** button to restart the system so that the changes can take effect.

**Remote Management**

HTTP Port  (Standard=80)

TELNET Port  (Standard=23)

(Enter 0 to disable remote management)

*Note: Changes made will only take effect after rebooting.*

#### Remote Management (continued...)

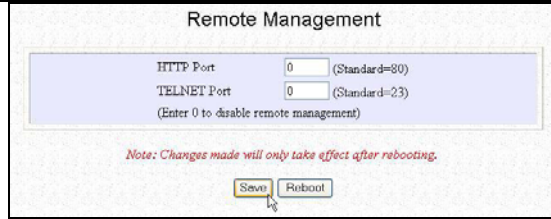
If you want to disable the

### Remote Management feature:

Key in **0** for both the **HTTP Port** and the **TELNET Port**.

Click on **Save** button.

Press the **Reboot** button to restart your computer so that the changes can take effect.



The screenshot shows a web-based configuration page titled "Remote Management". It contains two input fields: "HTTP Port" with a value of "0" and "(Standard=80)" next to it, and "TELNET Port" with a value of "0" and "(Standard=23)" next to it. Below these fields is a note: "(Enter 0 to disable remote management)". At the bottom of the form are two buttons: "Save" and "Reboot". A red note at the bottom of the page states: "Note: Changes made will only take effect after rebooting."

### 5.7 Enabling Parallel Broadband (Only available in Gateway mode)

Netkrom AIR-BR500G/GH is equipped with **Parallel Broadband** technology, which translates into scalable Internet bandwidth as well as Load Balancing and Fail-Over Redundancy features.

Since there is no restriction to the type of broadband Internet account that a Netkrom AIR-BR500G/GH can connect to, your network may run with one Netkrom AIR-BR500G/GH on Cable Internet, while the rest connect to ADSL.

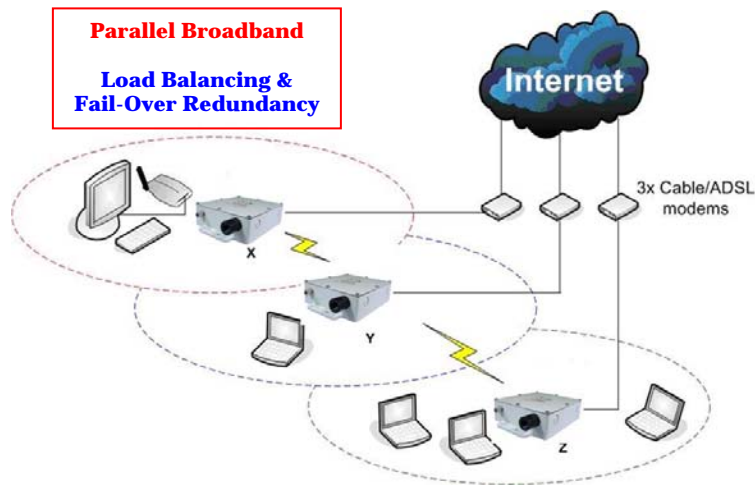
The diagram below illustrates an application of Parallel Broadband in a network with 3 Netkrom AIR-BR500G/GHs, **X**, **Y** and **Z**.

#### 5.7.1 Load balancing

Building your network around multiple Netkrom AIR-BR500G/GHs arranged in cascade and running under Parallel Broadband, creates an aggregate bandwidth and enables you to balance the Internet traffic generated by your private network over multiple broadband connections. For instance, **Z** might share its load with **X** and **Y** so that each Netkrom AIR-BR500G/GH serves approximately the same number of users.

#### 5.7.2 Fail-Over Redundancy

In case one of your broadband connections should fail, the affected Netkrom AIR-BR500G/GH will automatically switch over to other operational broadband channels so that your network is not disrupted. For instance, when the WAN connection to **Z** is down, **Z** will redirect its traffic to **Y**, and hence providing Fail-Over Redundancy of Internet access to wireless clients of **Z**.



To learn more about **Parallel Broadband**, please read the whitepaper at [www.netkrom.com](http://www.netkrom.com)

### 5.7.3 To enable Parallel Broadband

Before enabling the Parallel Broadband feature, verify whether:

- Each Netkrom AIR-BR500G/GH is correctly configured to connect to its specific broadband Internet account.
- You need to enable DHCP on all Netkrom AIR-BR500G/GHs in Parallel broadband. It is recommended that each Netkrom AIR-BR500G/GH leases IP in a non-overlapping IP address pool.
- All Netkrom AIR-BR500G/GH are interconnected in a chain manner using WDS as illustrated in the section on **WLAN Basic Setup**.
- Each Netkrom AIR-BR500G/GH is running in Gateway mode with the Parallel Broadband option enabled.

#### Enable Parallel Broadband

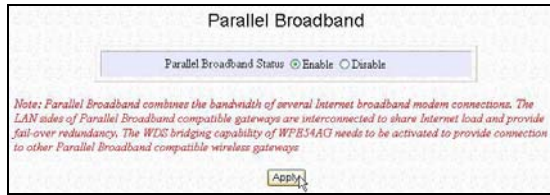
Click on **Parallel Broadband** from the **CONFIGURATION** menu.

By default the **Parallel Broadband** feature is disabled.

Enable the Parallel Broadband Status.

Click on **Apply** button.

Repeat this for the other Netkrom AIR-BR500G/GHs in your network.





### Chapter 6 System Utilities

This chapter provides guidelines in using:

- The SYSTEM TOOLS menu
- The HELP menu

#### 6.1 Using the SYSTEM TOOLS Menu

##### 6.1.1 System Identity

If your network operates with several Netkrom AIR-BR500G/GHs, you would find it useful to have a means of identifying each individual device.

In certain cases, your Internet Service Provider might request for a **System Name** before allowing you to access the Internet. This **System Name** also serves as a **DHCP Client ID** during negotiations with the DHCP Server for dynamic IP address allocation.

You can define the **System Identity** of Netkrom AIR-BR500G/GH to be also utilized as **System Name** or as **DHCP Client ID**.

**System Identity**

Click on **System Identity** from the **SYSTEM TOOLS** menu.

Enter the **DHCP Client ID** assigned by your ISP in the **System Name** field.

Fill in the name of a person to contact in the **System Contact** field.

Fill up the **System Location** field. If there are multiple devices in your network or building, this entry might help to identify the device.

Click on the **Apply** button to effect the changes.

System Identity

System Name	Wireless Access Point
System Contact	unknown
System Location	unknown

Apply Help

### 6.1.2 WLAN Station List (Only available in AP and Gateway mode)

This option allows you to view the wireless clients in the wireless network.

**WLAN Station List ( Available in AP mode)**

Click on **WLAN Station List** from the **SYSTEM TOOLS** menu.

Click on the **Refresh** button to get the latest information on the availability of wireless clients in the wireless network.

**WLAN Station List Show**

STA	MAC Address	State
STA0	00 0B 6B 47 FF C0	associated

**Refresh** **Back**

**WLAN Station List (Available in Gateway mode)**

Click on **WLAN Station List** from the **SYSTEM TOOLS** menu.

Click on the **Refresh** button to get the latest information on the availability of wireless clients in the wireless network.

**WLAN Station List**

ID	MAC Address	State	Signal	RSSI	rxRate
AP	00 80 48 2B E5 1D	up	-	-	-

**Refresh** **Back**

### 6.1.3 Set System's Clock

Synchronizing the built-in clock of Netkrom AIR-BR500G/GH with the time kept by your workstation will enable you to effectively manage and operate the time-based functions provided by Netkrom AIR-BR500G/GH.

**Set System's Clock**

Click on **Set System's Clock** from the **SYSTEM TOOLS** menu.

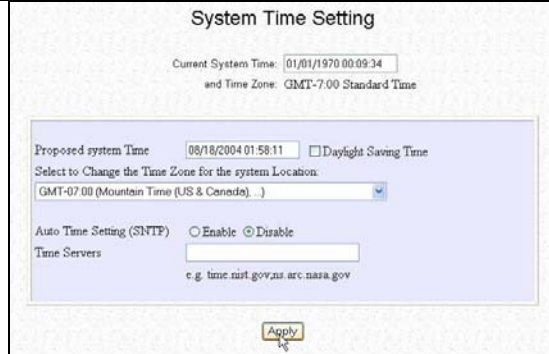
Select the appropriate time zone from the **Select to Change the Time Zone for the system Location** drop-down list.

Enable the **Auto Time Setting (SNTP)** radio button.

**SNTP** stands for Simple Network Time Protocol and is used to synchronise computer clocks in the Internet.

Fill in the **Time Servers** field.

Click on the **Apply** button to effect the changes



### 6.1.4 Firmware Upgrade

Netkrom products are designed for upgradeability. You can check the current version of your firmware by clicking on **About System** from the **HELP** menu.

Keep your Netkrom AIR-BR500G/GH updated with the latest capabilities by downloading its latest firmware revision from either of Netkrom's corporate web sites at [www.netkrom.com](http://www.netkrom.com) before following the next steps.

To begin with, ensure that you have downloaded the latest firmware onto your local hard disk drive.

#### Firmware Upgrade

Click on **Firmware Upgrade** from the **SYSTEM TOOLS** menu.

Key in the path and file name of the downloaded file in the **Upgrade Firmware (path and file name)** field.

Alternatively, click on the **Browse** button to locate the file.



Click on the **Upgrade** button.

Follow the instructions given during the upgrading process.

**Reboot** the system.



### NOTE

The firmware upgrade process must **NOT** be interrupted otherwise the device might become unusable.

### 6.1.5 Save or Reset Settings

You may choose to save the current configuration profile, to make a backup of it onto your hard disk, to restore an earlier profile saved on file or to reset Netkrom AIR-BR500G/GH back to its default settings.

#### Save Your Settings

Click on **Save or Reset Settings** from the **SYSTEM TOOLS** menu.

Click on the **Save** button.

**Reboot** the system.

Save the System's current configuration



#### Backup Your Settings

If you want to back up the current settings of your Netkrom AIR-BR500G/GH onto your hard disk drive:

Click on the **Backup** button.

Backup the System's configuration



### Restore Your Settings

Or you may directly type in the path name of the file at **Restore the Machine's configuration (path and file name)**.

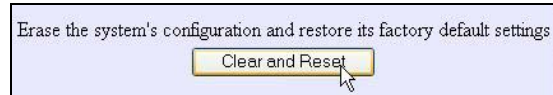
Click on the **Restore** button.



### Reset Your Settings to Factory Default

To discard ALL the configuration you have made and restore Netkrom AIR-BR500G/GH to its initial factory settings:

Click on **Clear and Reset** button.



#### 6.1.6 Reboot System

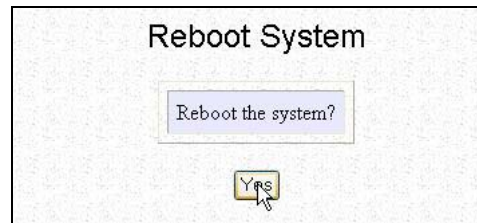
Most of the changes you make to the system's settings require a system reboot before the new parameters can take effect.

### Reboot Your device

Click on **Reboot System** from the **SYSTEM TOOLS** menu.

You will be prompted to confirm whether to execute a system reboot.

Click on the **Yes** button whenever you are ready to restart.



### 6.1.7 Change Password

It is recommended that you change Netkrom AIR-BR500G/GH login password, which is case sensitive and is set by default, to **password**.


**Changing your Password**

Click on **Change Password** from the **SYSTEM TOOLS** menu.

Key in the **Current Password**.  
The factory default is *password*.

Enter the **new password** in the **New Password** field as well as in the **Confirm Password** field.

Click on the **Change Password** button.



### 6.1.8 Logout

To exit the Web interface, follow the next few steps.

1. Click on **Logout** from the **SYSTEM TOOLS** menu.

Click the **Logon** button to access Netkrom AIR-BR500G/GH's configuration interface again.

### 6.2      Using the **HELP** menu

#### 6.2.1      Get Technical Support

This page presents the contact information of Netkrom's technical support centres around the world.

Get Technical Support
Click on <b>Get Technical Support</b> from the <b>HELP</b> menu.
Netkrom AIR-BR500G/GH is a feature-packed device. If you require further information than provided in the manual or data sheet, please contact one of Netkrom's Technical Support Centres by mail, email, fax or telephone.

#### 6.2.2      About System

The **About System** page displays a summary of your system configuration information. Support technicians might require specific information about your system data when they are troubleshooting your configuration. You can use the information displayed in this page to quickly find the data they need to resolve your system problem.

Get Technical Support
Click on <b>About System</b> from the <b>HELP</b> menu.
The <b>System Information</b> page will supply information concerning Netkrom AIR-BR500G/GH's configuration settings.

#### AI Solutions to Common Problems

In this section, we list suggested steps to rectify some common problems that may arise during the installation and operation of Netkrom AIR-BR500G/GH. If you do not find an answer here, you may also visit the corporate Netkrom website at [www.netkrom.com](http://www.netkrom.com).

1. **I want to know whether Netkrom AIR-BR500G/GH is connected to the Internet.**

A. Open a Command Prompt

For *Windows 98/98SE/ME*, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **command**. Press the **Enter** key or click the **OK** button.

For *Windows 2000 and XP*, please click the **Start** button and **Run**. In the **Open** field within the **Run** dialog box, type in **cmd**. Press the **Enter** key or click the **OK** button.

B. In the Command Prompt, type `ping 192.168.168.1` and press the Enter key.  
You will get a reply if the PC is communicating with the Netkrom AIR-BR500G/GH Access Point.

If you do NOT get a reply, ensure that your settings are correct before trying again. Your computer MUST be in the same subnet as Netkrom AIR-BR500G/GH.

C. In the Command Prompt, type `ping www.netkrom.com` and press the **Enter** key.

Obtaining a reply means that you are connected to the Internet.

Otherwise, you may want to ping another known host.

Getting no reply from any of the other hosts that you have tried, suggests that your connection may be having problems.



### 2. I am not getting an IP address and am unable to surf the Internet.

- A. Make sure that the Ethernet cable is properly connecting your Cable/ADSL modem to the WAN port of the Netkrom AIR-BR500G/GH access point, and verify whether the gateway has a valid IP address from the **About System** page. Then refer to suggested steps A, B & C to Problem 1 described above, to verify the connectivity of the gateway.
- B. Ensure that the WAN settings are relevant to your broadband connection. In case of doubt, you should contact your network administrator/ISP to enquire about your Internet connection type.
- C. Power off your computer, the Netkrom AIR-BR500G/GH access point and the Cable/ADSL modem. Turn on the Cable/ADSL modem then wait for 1 minute before turning on the gateway. Lastly, turn on your computer. Verify whether you have been allocated an IP address and are able to surf the web.

### 3. I am not able to access the Web interface of Netkrom AIR-BR500G/GH

- A. Refer to Problem 1 and follow suggested steps A and B to verify your connectivity to the Netkrom AIR-BR500G/GH access point.
- B. If you are a PPPoE user, you will need to remove the proxy settings or the dial-up pop-up window.
- C. If you are not using the uConfig utility, you may need to change the settings of your Web browser.

#### For Microsoft Internet Explorer 5.0 or later versions

From the **Tools** menu bar, select **Internet Options** and then click on the **Connections** tab. Click on the **LAN Settings** button. Uncheck any options from that dialog box. Press the **OK** button to return to the previous screen.

For PPPoE users, click the radio box option **Never dial a connection** to remove any dial-up pop-ups. Press the **OK** button to finish.

#### For Netscape 4.7 or later versions

Start Netscape Navigator. From the **Edit** menu bar, select **Preferences**, then **Advanced**, and finally **Proxies**.

Make sure that the **Direct connection to the Internet** option is selected.

Close all windows to finish.

4. **I want to set Netkrom AIR-BR500G/GH to its factory default settings.**

- A. Power up the gateway.
- B. Depress the **Reset** button situated at the back of the device and hold it for **2 to 10** seconds before releasing it.

5. **My laptop is not able to access Netkrom AIR-BR500G/GH.**

- A. In the Command Prompt, type ping 192.168.168.1 and press the Enter key.

If you get a reply, your laptop is communicating with the gateway.

If you do NOT get a reply, please continue with the following steps.

- B. Ensure whether your wireless card and driver have been properly installed.

Open the **Control Panel**. Double-click the **System** icon. Inside the **Device Manager** window, expand the **Network Adapters** listing and verify whether the name of your wireless card is listed.

If it does not, power down your laptop. Remove the wireless card from its slot and re-insert it, ensuring that it properly fits into the slot. Reboot your computer.

If it does, click on it and press the **Properties** button. Check whether **Device Status** displays this message “*This device is working properly*”. If it does not, you will need to uninstall and re-install the software driver.

- C. Verify whether your Netkrom AIR-BR500G/GH gateway and your laptop and/or other wireless clients have been configured with the same SSID, which is the case-sensitive name of the wireless network that you are trying to access, and the same WEP settings.
- D. Check whether your Netkrom AIR-BR500G/GH gateway and your laptop are using the same frequency channel.

6. **My network contains several Netkrom AIR-BR500G/GHs but they are unable to connect to each other.**

A. If you are running the **Parallel Broadband** feature:

Though they may belong to different SSIDs, the gateways **MUST** operate in the same frequency band.

B. If you are trying to implement a **WDS**:

Verify that the gateways are functioning in the same frequency band.  
Check whether the MAC address that you have added as WDS link corresponds to the wireless MAC address displayed in the **About System** page of your gateway.

### Appendix II Firmware Recovery

This section demonstrates how to reload the firmware to Netkrom AIR-BR500G/GH should the system fail to launch properly. In such cases, Netkrom AIR-BR500G/GH will automatically switch to loader mode and the **DIAG** LED will light up and remain ON.

Table 1 below illustrates the behaviour of the **DIAG** LED.

Netkrom AIR-BR500G/GH Operation State	DIAG LED
Corrupted firmware – Netkrom AIR-BR500G/GH switches to loader mode	Blinks very fast
Recovery in progress	ON
Successful recovery	Blinks very slowly

#### AII How to recover Netkrom AIR-BR500G/GH from failed firmware

Before starting, check the status of the **DIAG** LED against Table 1 above to verify whether firmware failure has occurred.

1. Power Netkrom AIR-BR500G/GH off and disconnect it from the network.
2. Use a MDI cable (cross-connect for Netkrom AIR-BR500G/GH) to connect the LAN port of Netkrom AIR-BR500G/GH to the LAN port of your computer.
3. Power Netkrom AIR-BR500G/GH on, and then start up your computer. The computer will obtain an IP address of **192.168.168.100** from Netkrom AIR-BR500G/GH.
4. Insert Netkrom AIR-BR500G/GH Product CD into the CD drive of your computer.
5. From the computer, click **Start**, then **Run** and type in the following command:

**X:TFTP -i 192.168.168.1 PUT X:image\_name.IMG**, where X refers to your CD drive and **image\_name.IMG** to the firmware filename found in the Recovery folder of the Product CD.

6. If you have downloaded a newer firmware and have saved it in your local hard disk as for example, **C:\netkrom\xxxx.IMG**, then replace **X:image\_name.IMG** with this new path and firmware name.
7. The recovery process will now take place. You can check the **DIAG** LED against Table 1 to monitor the progress of the recovery process.

## **Appendix II    Firmware Recovery**

---

8. When firmware restoration has completed, reboot Netkrom AIR-BR500G/GH and it will be ready to operate

